Tunable Reliability of Information Transport in Wireless Sensor Networks

Vom Fachbereich Informatik der Technischen Universität Darmstadt
genehmigte

Dissertation

zur Erlangung des akademischen Grades eines Doktor-Ingenieur (Dr.-Ing.)
vorgelegt von

M.Eng. Faisal Karim Shaikh

aus Matiari, Pakistan

Referenten:
Prof. Neeraj Suri, Ph.D.
Prof. Jörg Hähner, Ph.D.

Datum der Einreichung: 08. April 2010
Datum der mündlichen Prüfung: 01. Juni 2010

Darmstadt 2010
D17

Abstract

A key functionality of Wireless Sensor Networks (WSNs) consists in obtaining and transporting the information of interest (e.g., event/status) required by the applications. The applications running on WSN also specify desired reliability levels on the desired information. Consequently, reliability requirements, possibly changing over time and of tunable levels over an application, are stipulated on the transport of information. As the WSN environments are often exposed to perturbations (e.g., energy depletion, sensor and connectivity loss etc), these specifically need to be considered in order to achieve the desired reliability on information transport. The existing approaches to reliable transport typically focus on maximizing the attained reliability levels than the more complex facets of reliability adaptation or tunability. These approaches thus tend to over utilize the network resources (e.g., energy) even when the application does not require enhanced reliability. On this background, this thesis develops a novel generalized framework for reliable information transport in WSNs. The proposed framework supports various applications, provides tunable reliability of information transport and copes with dynamic network conditions.

To ascertain the fundamental issues dictating the reliability of information transport in WSNs, this thesis models and compares existing information transport techniques. We highlight the key problems with the existing techniques and provide solutions to achieve desired application requirements.

The generic information transport framework developed in this thesis comprises of flexible and modular architectural blocks where different existing approaches can be easily incorporated. To maintain the generality of the framework we classify WSN applications and devise their information model. We achieve tunable reliability using probabilistic forwarding and opportunistic suppression of the information. For the detection of information loss, a hybrid acknowledgement technique is proposed which efficiently combines implicit and explicit acknowledgments. To ensure end-to-end reliability we develop heuristics to allocate reliability across the hops and tunable retransmission mechanism at each sensor node. In addition, if the sensor nodes know the spatial correlation of the information, they adapt the number of retransmissions according to the number of source nodes. Furthermore, congestion control is necessary in order to ensure the tunable reliability. We propose proactively detecting the congestion by observing the input and output information flow across a node. When congestion is detected, we propose mechanisms to split the information flow on multiple paths to alleviate congestion. If the congestion persists the information rate is adapted by the sensor nodes.

Our simulation results in the standard sensor network simulator TOSSIM show that the proposed framework supports various applications with evolving reliability requirements, copes with dynamic network properties and outperforms the state-of-the-art solutions. Our framework also significantly reduces the number of transmissions to result in an efficient solution.

Kurzfassung

Eine wesentliche Funktion drahtloser Sensornetze (Wireless Sensor Networks, WSN) besteht darin, applikationsrelevante Informationen (etwa Ereignisse oder Zustandsinformationen) zu erfassen und zu übertragen. An diese Informationen, ihre Verarbeitung und ihre Übertragung spezifizieren WSN-Anwendungen unterschiedliche und sich im Laufe der Zeit verändernde Zuverlässigkeitsanforderungen, die wesentlich über die Umsetzung der Informationsübertragung realisiert werden. Im Laufe ihres Betriebs sehen sich WSN mit einer Vielzahl operationaler Störungen (z.B. dem Verlust von Sensorik, Konnektivität oder adäquater Energieversorgung) konfrontiert, die im Hinblick auf Sicherstellung einer hinreichenden Zuverlässigkeit der Informationsübertragung zu berücksichtigen sind. Bestehende Ansätze zur Gewährleistung einer zuverlässigen Informationsübertragung in WSN haben die Maximierung der Zuverlässigkeit zum Ziel. Sie ignorieren dabei die Variabilität der Zuverlässigkeitsanforderungen und erreichen dadurch eine Überapproximation der realen Anforderungen, die eine teils unnötig überhöhte Belastung der Systemressourcen (z.B. in Form erhöhten Energiebedarfs) zur Folge hat, sobald die maximal erzielte Zuverlässigkeit den real erforderlichen Grad an Zuverlässigkeit übersteigt. Vor dem Hintergrund dieser Problematik beschreibt die vorliegende Arbeit einen neuartigen generalisierten Ansatz zur Umsetzung zuverlässiger Informationsübertragung in WSN. Der präsentierte Ansatz ist für verschiedenartige WSN-Applikationen anwendbar, bietet justierbare Zuverlässigkeit der Informationsübertragung und berücksichtigt sich dynamisch verändernde operationale Bedingungen des Netzwerks.

Die vorliegende Arbeit modelliert und vergleicht bestehende Umsetzungen der Informationsübertragung, um entscheidende Faktoren bei der Sicherstellung seiner Zuverlässigkeit zu identifizieren. Wir zeigen die wesentlichen Probleme dieser Ansätze auf und präsentieren Lösungen zur Umsetzung anwendungsspezifischer Zuverlässigkeitsanforderungen.

Der in der vorliegenden Arbeit entwickelte generische Ansatz für die Informationsübertragung besitzt einen modularen Aufbau, der einen flexiblen Austausch seiner Komponenten (etwa zur Integration bestehender alternativer Mechanismen) ermöglicht. Die Generizität des Ansatzes wird sichergestellt, indem WSN-Anwendungen klassifiziert werden und die Informationsmodelle dieser verallgemeinerten WSN-Anwendungsklassen abgeleitet und den präsentierten Betrachtungen zugrunde gelegt werden. Wir erzielen justierbare Zuverlässigkeit durch die Kombination zweier Techniken: Probabilistic Forwarding und Opportunistic Suppression zu übertragender Information. Zur Erkennung von Informationsverlusten bei der Übertragung wird ein hybrider Acknowledgement-Mechanismus vorgeschlagen, der implizite und explizite Acknowledgements effizient kombiniert. Um Zuverlässigkeit durchgängig über sämtliche Stufen der Informationsübertragung sicherzustellen, werden Heuristiken zur Assoziation von Zuverlässigkeit zu atomaren Teilstrecken drahtloser Übertragung (Hops) und justierbare Mechanismen zur wiederholten Übertragung für Knoten des WSN entwickelt. Sofern Sensor-

knoten über Wissen zur räumlichen Korrelation zu übertragender Information verfügen, passen sie die Anzahl wiederholter Übertragungen an die Anzahl der Ursprungsknoten dieser Information an. Eine weitere Voraussetzung justierbarer Zuverlässigkeit ist Congestion Control, das in dieser Arbeit in einem proaktiven Ansatz durch Überwachung des an Sensorknoten ein- und ausgehenden Informationsflusses realisiert wird. Falls ein Congestion-Zustand erkannt wird, werden Mechanismen zur Aufteilung des Informationsflusses über mehrere Pfade aufgezeigt, die diesem Problem entgegenwirken. Für den Fall, dass der Congestion-Zustand dennoch weiterhin besteht, wird eine Adaption der Übertragungsrate vorgenommen.

Die mit dem Sensornetz-Simulator TOSSIM erzielten Simulationsergebnisse zeigen, dass der in dieser Arbeit entwickelte Ansatz eine Reihe unterschiedlicher Anwendungen mit sich entwickelnden Zuverlässigkeitsanforderungen unterstützt, flexibel auf sich verändernde operationale Bedingungen des Netzwerks reagiert und, in der Kombination dieser Eigenschaften, bestehende Lösungen übertrifft. Der präsentierte Ansatz reduziert ferner die Anzahl erforderlicher Übertragungen beträchtlich, um eine effiziente Lösung des betrachteten Problems sicherzustellen.

Acknowledgements

Starting with the name of ALLAH, most gracious, most merciful.

I would probably not have made this far without the help, guidance and support of many people.

First and by far most, I wish to thank Prof. Neeraj Suri, my advisor and mentor, for first accepting me in DEEDS group, and then guiding me to where I am now. He taught me how to undertake the research and scientific challenges. Not only this, but how to present the results by polishing and improving my writing skills. He was always patient and helpful whenever his guidance and assistance was needed. Thanks for all this, *Neeraj*!

My gratitude to my colleague and friend, Abdelmajid Khelil (Majid) is enormous. Majid has been a constant source of inspiration and help since he joined the group. We had very interesting and fruitful discussions over the times. A great many thanks also to Prof. Jörg Hähner for accepting to be my co-advisor.

Time passes fast, it seems like I just arrived in Germany. It is all because of the love and fun environment at DEEDS group. Many thanks to *Azad, Brahim, Dan, Dinu, Daniel, Hamza, Matthias, Peter, Piotr, Sabine, Stefan, Thorsten, Ute* and *Vinay*, for being around and creating good working environment. I will be missing you all! The memories of former colleagues are always cherishing, *Andina, Andreas, Birgit, Boyan, Marco* and *Ripon*, guys you are great!

My sincere and heartfelt thanks go to my parents, *Fazal Karim Shaikh* and *Mumtaz Shaikh*, who were always there when I needed them. Their constant moral support has been very encouraging all these years. I also thank my brother, *Farhan*, and sisters, *Mona* and *Hifza*, for their endless love.

In last, saving the best for my lovely and sweet wife, *Shumaila*. Thank you for your support, your love, your patience and everything!

Not to mention, *Eshaal* - a cute angel, who has given a complete new meaning to my life. Papa loves you!

Contents

List of Figures

List of Tables

Chapter 1

Introduction

The fusion of sensing and wireless communication has developed into a the research field of Wireless Sensor Networks (WSNs). Recently, WSNs have been proposed for multiple applications, such as fire detection [Guang-Hui et al., 2006; Hartung et al., 2006], object tracking [Shih et al., 2008] and environmental monitoring [Selavo et al., 2007]. The commercial use of WSNs is expected to increase dramatically in the near future.

Generally, a WSN comprises of a large number of static sensor nodes possessing low processing, limited power capabilities and often communicating over short-range unreliable radio links. Additionally, sensor nodes have limited storage capacity and multiple onboard sensors such as temperature, humidity and accelerometers. Sensor nodes are deployed in an ad-hoc manner and cooperate with each other to form a wireless network. Since the communication range of sensor nodes is limited, hop-by-hop communication is adopted by sensor nodes to exchange data. Typically, a powerful base station termed as *sink*, is also an integral part of a WSN. The sink mediates between the sensor nodes and the applications running on a WSN. WSNs offer significant advances over traditional wired sensing networks and can be applied in many scenarios because of their flexibility, cost-effectiveness and ease of deployment. With the rapid emergence of WSN applications, WSNs are becoming an integral part of ubiquitous and pervasive systems, grid systems (e.g., SensorGrid [Fox et al., 2008; Lim et al., 2005]) and web services (e.g., Sensor Web [Delicato et al., 2003]).

Many WSN applications are data centric, i.e., they are deployed to interact with the physical environment and report the phenomenon of interest to the user via the sink. Therefore, the main functionality of a WSN is to support the transport of data generated in response to the sensed phenomenon towards the sink. One of the possibility is to send all the generated sensor data to the sink. Once the data is available at the sink, the users/applications

can infer their desired information. As the communication over radio is a dominant energy consuming operation [Akyildiz et al., 2002], it is highly inefficient to send the raw data to the sink. A commonly advocated approach to meaningfully process the raw data is utilizing distributed in-network preprocessing operations such as *filtering* and *aggregation*. After processing the raw data, the sensor nodes can deduce information locally, e.g., by using threshold techniques [Hellerstein et al., 2003]. Accordingly, we define *information* as the meaningful interpretation of the raw data within the network for transportation towards the sink.

With the evolution of WSNs, many applications are supported to run concurrently [Yu et al., 2006]. The applications running on WSNs stipulate their specific information (event/status) requirements from the network. As the applications are interested in the information generated in the network, reliably transporting the desired information is a key requirement in WSNs. Basic network routing provides the paths between sensor nodes and the sink for the information delivery. The routing strategies alone are not sufficient to provide information transport reliability since their primary objective is to find suitable routes. Thus, ensuring the reliable transport of information requires other mechanisms to be developed on top of readily available basic solutions.

Typically, WSNs utilize intrinsic sensor node redundancy for assuring proper network connectivity such that all senor nodes can communicate with the sink in a multihop fashion. However, the redundancy of sensor nodes comes at a cost. The redundant nodes generate correlated information and delivering the same information from multiple sensor nodes rapidly depletes the energy resources in the network. Furthermore, different applications running on WSNs demand various types of information with diverse reliability requirements. For example, a critical event detection application may require high reliability of event delivery. Alternatively, a non-critical monitoring application can tolerate some loss of information. Varying application requirements impose consequent reliability obligations to the base information transport in a WSN. In addition, the same WSN application may change its requirements over time [Kuorilehto et al., 2005]. Thus the reliability of information transport should be tuneable according to the types of information and application requirements.

Being an ad-hoc environment, WSN is subject to a wide range of operational perturbations affecting the transport of information to the sink. The major reasons for information loss in WSNs include collisions, contention and congestion. Along with node and communication perturbations, environmental disturbances also contribute to the loss of information. These perturbations naturally lead to deviation between the attained and the de-

sired reliability of information transport. If the attained reliability is higher than required, the information transport wastes valuable resources in the network. Conversely, if the attained reliability is lower than desired, the information usefulness for the application is compromised.

The remainder of this chapter is organized as follows. First, we highlight the problem being addressed in this thesis. Next, the main ideas driving the research in this thesis are presented. Later, we summarize the thesis goals in terms of research questions followed by the answers in the form of research contributions of this thesis.

1.1 Problem Statement

In WSNs, the in-network processing for inferring information leads to the generation of information as close to source nodes as possible. In this thesis, we focus on the core functionality of generic information transport in WSN deployments while assuming an accurate information generation.

Some applications may be interested in acquiring the information periodically while others may be interested in getting the information when some phenomenon of interest has occurred in the network. Accordingly, the generated information may also have a spatial correlation corresponding to the phenomenon of interest. For example, in case of fire detection application more than one sensor nodes detect the fire and report the information to the application. In literature, we find various works for generating and inferring in-network information [Ali et al., 2010; Fasolo et al., 2007; Oka and Lampe, 2008]. On the contrary, to the best of our knowledge there is no research that manages the generated information, i.e., manages the redundancy of information and selects the appropriate sensor nodes according to application requirements. For the information transport it is necessary to manage information in an appropriate way such that minimal resources are consumed without compromising the application requirements.

Despite a wide range of perturbations, the applications running on top of WSNs require certain reliability to deliver the desired information. The application requirements impose subsequent reliability constraints for the information transport in a WSN. There has been intensive research to design transport protocols for providing reliability guarantees [Ganesan et al., 2001; Stann and Heidemann, 2003; Zhang et al., 2005]. The existing efforts mitigate perturbations to some extent, however, are not able to cope with evolving and dynamic network conditions as they are designed for specific applications and perform well only for carefully selected scenarios [Shaikh et al., 2008].

A particular perturbation for information transport is the occurrence of

network congestion. Congestion typically manifests when many sensor nodes generate a burst of information and send it simultaneously to the sink. Congestion also prevents the maintaining of the desired application reliability. Therefore, the information transport should cope with congestion in an appropriate way such that the application requirements are fulfilled. The existing approaches [Chen and Yang, 2006; He et al., 2008; Hull et al., 2004a; Jaewon et al., 2007; Vuran et al., 2005; Wan et al., 2003] explicitly tackle congestion and are reactive in nature leading to information loss before some action can take place. These solutions assume that congestion is the only reason hindering the reliable information transport. The recent surveys [Rahman et al., 2008; Wang et al., 2006a] suggest to cope with congestion alongside other perturbations and provide reliability for information transport.

To this end very few strategies favor hybrid solutions by considering reliability guarantee and congestion control together [Paek and Govindan, 2007; Sankarasubramaniam et al., 2003]. However, the existing solutions are not designed to explicitly consider variable application requirements as their main design driver is to efficiently maximize the attained reliability. The existing approaches over-utilize the WSN resources (e.g., energy) even when the application does not require that level of reliability. Therefore, tunable information transport reliability is vital which provides the application specific reliability, adapts according to network conditions and pro-actively mitigates the congestion.

Figure 1.1 depicts the design space with respect to network conditions and reliability. The figure highlights the regions, where the existing solutions are likely to operate well. The design of a solution that covers the entire depicted space presents the main objective of the research in this thesis.

To the best of our knowledge, there exists no solution which manages the redundancy of information in the network, satisfies the varying application requirements and copes with dynamic network conditions simultaneously.

The deployment of one of the existing solutions on sensor nodes, limits the operational conditions under which sensor nodes can transport information reliably. For example, an existing solution which provides high reliability will consume resources unnecessarily even when applications do not require high reliability. Similarly, if we deploy a solution which handles only a subset of perturbations, e.g., link losses, the information transport is unsuccessful in scenarios where other perturbations such as congestion occur. If the congestion prevailed then such a solution will fail hampering information transport. Thus, for a generic WSN the existing solutions are not sufficient. Therefore, necessitating a framework which takes care of all possible situations. Such an integrated approach should maximize the supported operating conditions and provide efficient mechanisms to maintain the application reliability require-

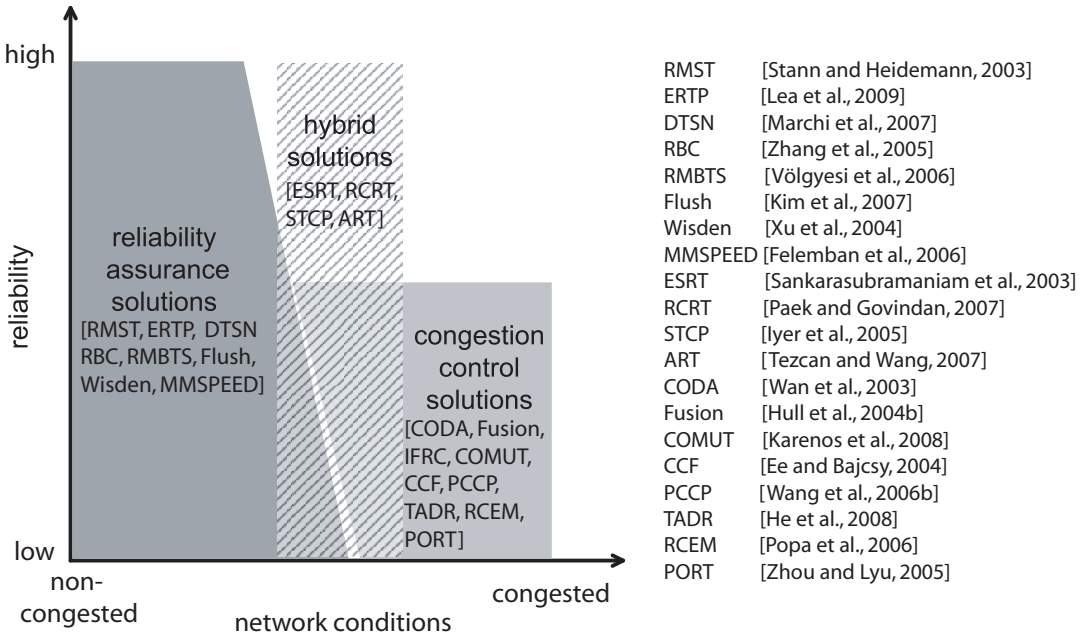


Figure 1.1: Related work design space

ments, i.e., minimum number of messages should be exchanged to maintain the desired reliability.

Our approach is to design an adaptable solution which provides necessary tools to support generalized applications in a decentralized manner. We propose a modular architecture that keeps the generality of the framework intact by allowing different modules to adapt and reuse the existing mechanisms. The framework provides best-effort latency for information transport, i.e., does not explicitly consider the timeliness. The framework contributes towards reduction of the end-to-end latency by managing information redundancy, mitigating perturbations and reducing the number of transmissions.

In this thesis, we propose the solutions for supporting tunable reliability of information transport in WSNs. The specific contributions of the thesis are as follows:

- Modeling and comparison of existing information transport protocols.

- Generic information transport framework for tunable reliability in WSNs.

1.2 Analytical Modeling and Comparison of Information Transport Protocols

In order to understand the basics and to explore the problem space of information transport, the first contribution of the thesis is to model and compare the existing information transport mechanisms. Currently, there are very few analytical works on reliability of information transport in WSNs. This is due to the volatile nature of WSNs which complicates the modeling of huge number of sensor nodes. Most of the conducted analytical research work aims at the investigation of the sensor node modeling [Bein et al., 2005] or modeling of clustered WSNs [AboElFotoh et al., 2005; Shrestha et al., 2007; Xing and Shrestha, 2006] or reliability of the whole WSN [Vinga, 2009] but none for the reliability of information transport.

In order to establish the analytical models for reliability of information transport in WSNs, we consider solutions from the area of systems reliability, where the reliability of whole system is modeled at the level of functional components while their implementation details are bypassed for the sake of simplicity. One such example is to utilize reliability block diagrams (RBD) where the reliability of the system is modeled at the abstract level. We show how to utilize RBD models for the information transport reliability in WSNs.

Furthermore, along with the analytical model, we present the first simulation based comparative study concerning the performance of existing transport protocols for WSN. We simulate a wide range of network dynamics and show that existing protocols are not able to (a) cope with evolving network conditions and (b) fulfill application requirements. The simulation study also motivates the necessity and usefulness of the adaptation of protocols to the dynamic and evolvable network conditions. The comparative study represents an important step in understanding the performance of various transport protocols and highlights the limitations of existing techniques.

1.3 Framework for Tunable Reliability of Information Transport

After establishing the fact that the existing solutions are not able to cope with evolving application requirements and dynamic network conditions, we develop a framework for information transport in WSNs. The framework comprises four modules: information, tuning & adaptation, reliability and network monitoring. The framework consists of a flexible architecture where different approaches can easily be incorporated. We develop the basis for

different modules of the framework and show the efficient interactions among them.

The information module of the proposed framework provides (a) abstraction for the different types of information, and (b) provides efficient solutions for managing the information in the network.

We develop mechanisms utilized by the reliability and tuning & adaptation modules of the proposed framework. The developed mechanisms exploit spatial correlation of the information and temporal redundancies in the WSNs. Consequently, we design and evaluate the technique for exploiting the spatial correlation of the information. We achieve tunable reliability using probabilistic forwarding and suppression of the information. For recovering from information loss, a hop-by-hop implicit acknowledgment scheme is employed. To ensure end-to-end reliability, we introduce adaptive retransmission mechanisms at each sensor node. In addition, the sensor nodes adapt the number of retransmissions according to the number of source nodes generating the information.

For fulfilling the desired application reliability requirements we develop a mechanism to allocate the reliability along the path. Since getting the global knowledge of complete path is inevitable, we propose a localized heuristic for reliability allocation. The efficiency of our proposed mechanisms is validated by having a significantly reduced number of transmissions compared to the existing solutions. As a byproduct we also observe that the proposed mechanisms enhance the timeliness of information delivery of the existing approaches. Our simulation results show that exploiting the spatial redundancy results in increasing the efficiency of the information transport (i.e., reduce the number of transmissions).

Next, we argue that congestion control is necessary for providing and maintaining the tunable reliability. In order to provide tunable reliability and to mitigate congestion in WSNs, we develop an efficient technique comprising of two components: a hop-by-hop reliability component and a congestion control component. The reliability component allows tunable reliability by dynamically controlling the number of retransmissions at each intermediate node. For information loss recovery we propose a hybrid acknowledgement scheme, a unique and efficient combination of implicit and explicit acknowledgments. To determine how long the sensor node should wait for hybrid acknowledgement is non-trivial and depends on the time it takes for the information to be forwarded by the next node along the path. To overcome this, our solution utilizes adaptive retransmission timers by observing the information flow across the neighboring sensor nodes. The congestion control component allows tunable reliability in the face of congestion. We classify different forms of congestion in the network and proposes a pro-active con-

gestion detection mechanism by observing the input and output information flow across a node. By combining the tunable reliability and congestion control mechanisms, our proposed approach ensures the desired application reliability. Extensive simulations show that our proposed technique provides tunable reliability along with congestion control and outperform the existing solutions.

In order to enable the successful adaptation of the framework, the current network conditions have to be monitored. To acquire global network properties in WSNs is costly because of the high communication overhead for the sensor nodes. Therefore, we develop strategies which can estimate the global properties of WSN through local observations. The proposed localized strategies aid the functionality of network management module to efficiently collect the network properties.

We evaluate the entire framework and show that the proposed framework outperforms the existing solutions and in some cases four to five times reduction of transmissions is achieved for information transport.

1.4 Summary

In this section we briefly revisit the research goals in the form of research questions and summarize the thesis contributions.

1.4.1 Thesis Research Questions

The research questions driving the research presented in this thesis consider the different aspects of achieving and maintaining tunable information transport reliability.

Research Question 1 (RQ1): *How to model the reliability of information transport in WSNs?*
Chapter 3 sets up the modeling technique for reliability of information transport in WSNs. The modeling technique must be general enough to represent the majority of transport protocols despite the inherent dynamic network conditions.

Research Question 2 (RQ2): *Why are the existing approaches insufficient for reliable information transport in WSNs?*
Chapter 3 raises and answers this research question while discussing the various aspects of application scenarios and dynamic network conditions, and demonstrates that the current approaches are insufficient.

Research Question 3 (RQ3): *Is it possible to develop a generic solution for information transport in WSNs?*
Chapter 4 discusses the various aspects for a generic solution and focuses on different characteristics it should provide. Consequently, a generic information transport framework is developed. In Chapter 7 we evaluate the proposed framework and show its validity.

Research Question 4 (RQ4): *How is the information represented and managed in WSNs?*
Chapter 2 discusses the different types of information generated in a WSN and provides an abstract information classification for the information transport. Chapter 4 discusses the various strategies for managing the information in WSNs.

Research Question 5 (RQ5): *How to achieve tunable reliability of information transport in WSNs?*
The ability to accurately answer this question is crucial for ensuring the adequacy of information transport reliability. Chapter 5 addresses this question by introducing and then discussing the conceptual basis for tunable reliability and highlighting the achieved gains.

Research Question 6 (RQ6): *How does the spatial correlation of information aid the tunable reliability of information transport?*
Chapter 5 discusses this issue and provides basis for exploiting the spatial correlation.

Research Question 7 (RQ7): *How the information transport should deal with congestion in the network?*
In Chapter 6, these questions are answered by presenting the efficient solutions for recovering from different types of congestion.

1.4.2 Thesis Contributions

Now we summarize the main contributions which also represent answers to the above raised research questions.

Contribution 1 (C1) – Modeling and Comparison: We show that the complex mechanism of information transport in WSNs can be tackled in an abstract way yet keeping the relevant aspect of information transport intact. Next, we compare the existing solutions using simulation and highlight the areas where they perform unsatisfactory. (RQ1, RQ2)

Contribution 2 (C2) – Tunable Reliability Framework: We propose a flexible and modular framework for tunable reliability of information transport. The framework is evaluated using the widely accepted simulator TOSSIM thus validating its applicability and usefulness. (RQ3, RQ4, RQ5, RQ6, RQ7)

Contribution 3 (C3) – Information Classification and Management: An abstract information classification is proposed to represent different types of information required by applications running on the WSNs. Accordingly, we proposed efficient in-network solutions for information management in WSNs. (RQ4)

Contribution 4 (C4) – Spatial Correlation and Tunable Reliability: We design a distinctive solution to provide tunable reliability by incorporating reliability allocation along the path and using adaptive retransmissions. Consequently, we design a solution which provides tunable reliability by adapting the number of retransmissions according to spatial correlation of the generated information. (RQ5, RQ6)

Contribution 5 (C5) – Proactive Congestion Control and Tunable Reliability: In order to provide the desired reliability of information transport in face of congestion we propose a unique proactive mechanism by monitoring the information flow across the sensor nodes. To recover from information loss we propose a hybrid acknowledgement scheme which efficiently combines well known implicit and explicit acknowledgement mechanisms. To ensure the viability of the proposed mechanism, we develop application level retransmission timer management. (RQ5, RQ7)

1.4.3 Publications Resulting from the Thesis

The work reported in this thesis is supported by several international peer-reviewed publications:

- **Faisal Karim Shaikh**, Abdelmajid Khelil, Azad Ali and Neeraj Suri, *ReCAIT: Reliable Congestion Aware Information Transport in Wireless Sensor Networks*, submitted to International Journal of Communication Networks and Distributed Systems, a Special issue "Scalable Wireless Networks", 2010. (under review)

- **Faisal Karim Shaikh**, Abdelmajid Khelil, Brahim Ayari, Piotr Szczytowski and Neeraj Suri, *Generic Information Transport for Wireless*

Sensor Networks, Proceedings of the third IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing (SUTC), June 2010. (to appear)

- **Faisal Karim Shaikh**, Abdelmajid Khelil, Azad Ali and Neeraj Suri, *TRCCIT: Tunable Reliability with Congestion Control for Information Transport in Wireless Sensor Networks*, Proceedings of the International Wireless Internet Conference (WICON), 2010.

- **Faisal Karim Shaikh**, Abdelmajid Khelil and Neeraj Suri, *AReIT: Adaptable Reliable Information Transport for Service Availability in Wireless Sensor Networks*, Proceedings of The International Conference on Wireless Networks (ICWN), pp. 75-81, 2009. (acceptance rate 25%)

- **Faisal Karim Shaikh**, Abdelmajid Khelil and Neeraj Suri, *A Comparative study of Data Transport Protocols in Wireless Sensor Networks*, Proceedings of IEEE International Symposium on World of Wireless, Mobile and Multimedia Networks (WOWMOM), pp. 1-9, 2008. (acceptance rate 17.7%)

- **Faisal Karim Shaikh**, Abdelmajid Khelil, Neeraj Suri, *Poster: Meeting the Evolving Reliability Requirements for WSN Applications* In Proceedings of European Conference on Wireless Sensor Networks (EWSN), 2007.

- **Faisal Karim Shaikh**, Abdelmajid Khelil, Neeraj Suri *On Modeling the Reliability of Data Transport in Wireless Sensor Networks*, In Proceedings of Euromicro Conference on Parallel, Distributed and Network-based Processing (PDP), pp. 395-402, 2007.

Additionally, the author has been involved in the following publications that are not directly covered by the thesis:

- Piotr Szczytowski, **Faisal Karim Shaikh**, Vinay Sachidananda, Abdelmajid Khelil and Neeraj Suri, *Mobility Assisted Adaptive Sampling in Wireless Sensor Networks*, In Proceedings of the International Conference on Networked Sensing Systems (INSS), Demo Session, 2010. (to appear)

- Abdelmajid Khelil, **Faisal Karim Shaikh**, Azad Ali, Neeraj Suri and Christian Reinl, *Delay-Tolerant Monitoring of Mobility-Assisted Wireless Sensor Networks*, In "Delay Tolerant Networks: Protocols and

Applications", Auerbach Publications, CRC Press, Taylor & Francis Group, Edited by A. Vasilakos, Y. Zhang, T. Spyropoulos (to appear 2010)

- Abdelmajid Khelil, **Faisal Karim Shaikh**, Azad Ali and Neeraj Suri, *gMAP: Efficient Construction of Global Maps for Mobility-Assisted Wireless Sensor Networks*, Proceedings of Conference on Wireless On demand Network Systems and Services (WONS), pp. 189-196, 2009.

- Abdelmajid Khelil, Christian Reinl, Brahim Ayari, **Faisal Karim Shaikh**, Piotr Szczytowski, Azad Ali and Neeraj Suri, *Sensor Cooperation for a Sustainable Quality of Information*, In "Pervasive Computing and Networking", John Wiley, Edited by Prof. Mohammad S. Obaidat and Dr. Mieso Denko (to appear 2010).

- Abdelmajid Khelil, **Faisal Karim Shaikh**, Piotr Szczytowski, Brahim Ayari and Neeraj Suri *Map-based Design for Autonomic Wireless Sensor Networks*, In "Autonomic Communication", Springer-Verlag, Edited by A. Vasilakos, M. Parashar, S. Karnouskos, W. Pedrycz (June 2009).

- Azad Ali, Abdelmajid Khelil, **Faisal Karim Shaikh** and Neeraj Suri *Efficient Predictive Monitoring of Wireless Sensor Networks*, In International Journal of Autonomous and Adaptive Communications Systems (IJAACS), INDERSCIENCE publishers. (to appear 2010)

- Azad Ali, Abdelmajid Khelil, **Faisal Karim Shaikh** and Neeraj Suri *MPM: Map based Predictive Monitoring for Wireless Sensor Networks*, 3rd International ICST Conference on Autonomic Computing and Communication Systems (AUTONOMICS), 2009.

- Matthias Krop , Arthur Herzog, Daniel Jacobi, Kim Listmann, Karen Petersen, Katayon Radkhah, Christian Reinl, **Faisal Karim Shaikh**, Armin Strobel and Oskar von Stryk *MM-ulator: Towards a Common Evaluation Platform for Mixed Mode Environments*, In Proc. of The International Conference on Simulation, Modeling, and Programming for Autonomous Robots (SIMPAR), 2008.

- Abdelmajid Khelil, **Faisal Karim Shaikh**, Brahim Ayari and Neeraj Suri *MWM: A Map-based World Model for Event-driven Wireless Sensor Networks*, In Proc. of The 2nd ACM International Conference on Autonomic Computing and Communication Systems (AUTONOMICS) 2008.

1.5 Thesis Structure

The rest of the thesis has the following structure:

Chapter 2 first presents the system model used throughout in this thesis. Next, we classify WSN applications and accordingly define the abstract information model. Subsequently, the perturbation and reliability models are presented. Finally, the experimental environment used for evaluating different approaches is discussed.

Chapter 3 classifies and surveys the state of the art and practice in the design of information transport techniques for WSNs. Correspondingly, Chapter 3 develops the modeling technique for information transport using reliability block diagrams. We show how the proposed analytical model can be utilized to adapt protocol parameters to WSN network characteristics. Then, we compare the existing information transport protocols using simulations for a wide range of operating conditions.

Chapter 4 introduces our generic information transport framework. First, we investigate the major considerations for the design of generalized solution through discussing the design requirements for information transport in WSNs. Next, we define and elaborate the modular architecture of the framework.

Chapter 5 depicts the advantages of exploiting the spatial correlation and investigates a methodology to maintain tunable reliability in the presence of communication perturbations.

Chapter 6 extends the approaches for achieving tunable reliability considering the wider range of perturbations including link loss, link congestion and buffer overflows.

Chapter 7 comprehensively evaluates the proposed framework for wide range of network conditions and for different types of information generated in the network.

Chapter 8 first provides the future research directions opened by the novel approach presented by this thesis. Next, we conclude the thesis by re-evaluating the contributions.

Chapter 2

Generalized Models

This chapter starts by presenting the generalized system model for WSNs. Given the continual increase in WSN applications and their requirements, we believe that a proper classification and characterization of applications is a prerequisite for information transport framework. Consequently, this chapter presents the WSN application classification and discusses their requirements for information transport. Based on the application classification an abstract information model is developed. The proposed information model corresponds to one of our contributions, i.e., **C3** (Section 1.4.2). Subsequently, the perturbation model is presented which covers the various failures encountered in the stated system model along with corresponding reliability model.

2.1 System Model

We consider the conventional model of a WSN having **N** sensor nodes and a single sink (S). Typically, each node is equipped with one or more sensing devices, short range transceivers with limited processing, memory and energy capabilities. We consider the sink to be adequate in power (ideally up to entire expected life of network), memory and processing capabilities as compared to the sensor nodes. We assume that all nodes are static in nature (including the sink). However, the topology of WSN is dynamic due to perturbations in the network. Each sensor node maintains a limited buffer of size Q. The sensor nodes communicate with each other via bi-directional multihop wireless links employing a CSMA-based Medium Access Control (MAC) protocol. For any two nodes X and Y we define their link quality $LQ = p_{(X,Y)} \cdot p_{(Y,X)}$, where $p_{(X,Y)}$ and $p_{(Y,X)}$ indicate the probability that a message sent by Node X is received correctly by Node Y and vice versa. X, Y are defined to be neighbors, if $LQ \neq 0$. This implies that IACK can be used in our model, since neighbors can always hear each other. Let the sequence of hops (X, H_1), $(H_1, H_2) \cdots (H_f, S)$ create a path $Path_i$ from Node X to the sink. All sensor nodes know their hop distance $h(X)$ from the sink and their one-hop neighbors. Based on hop distances, the neighbors of a node can be classified as upstream neighbors, downstream neighbors and equal neighbors.

Definition 1. *We denote the set* $N_u = \{Y : \{X, Y\} \in \boldsymbol{N} \wedge h(Y) = h(X)+1\}$ *as the upstream neighbors of a node* X*, the set* $N_d = \{Y : \{X, Y\} \in \boldsymbol{N} \wedge h(Y) = h(X) - 1\}$ *as its downstream neighbors, and the set* $N_e = \{Y : \{X, Y\} \in \boldsymbol{N} \wedge h(Y) = h(X)\}$ *as its equal neighbors respectively.*

We assume an underlying routing protocol, which provides a path to the sink for all nodes. Without loss of generality we assume that all paths end at the sink. We consider an underlying routing protocol which provides a sensor node with a next hop along the path to the sink. The sensor nodes generate message(s) corresponding to the information to form one-to-one or many-to-one convergent traffic in the upstream direction, i.e., from sensor nodes to the sink. A sensor node can be either a source node and/or relay node. In order to acquire the hop count $h(X)$ the sensor nodes may utilize the underlying routing protocol.

2.2 Application Classification

There is not a single solution which covers all the WSN applications. For different applications customized solutions are deployed. We classify the

different types of WSN applications and provide a set of corresponding requirements on information transport. Most of the current applications fall into one of the following classes.

Periodic/Continues applications: In this class of applications, each sensor node periodically generates data to be transported towards the sink. Different operations such as filtering and aggregation can be applied to the data on the fly. The data from sensor nodes can be aggregated to reduce the number of messages in the network. As the information can be received in subsequent rounds the reliability and timeliness requirements are flexible for this class of applications. Examples of periodic/continues WSN applications include environmental monitoring [Cerpa et al., 2001; Dinh et al., 2007; Selavo et al., 2007; Szewczyk et al., 2004].

Event detection applications: For such applications one or more sensor nodes generate the data and transport it towards the sink. In either case information is binary in nature, i.e., whether an event happened or not. Usually these applications require high reliability and low latency. Few examples of event transport applications are fire detection [Sankarasubramaniam et al., 2003] and enemy detection on battle field [Zhang et al., 2005], etc.

Tracking applications: For tracking applications [Chellappa et al., 2004; Shih et al., 2008] many sensor nodes track a target and transport location information towards the sink. The information is short lived and some losses can be tolerated by the applications. Depending on the application the reliability/latency requirement on information transport may vary.

Query based applications: These applications require a group of sensor nodes to generate one or more query results. The information can be single in nature or composed of sub-information. Query based applications are pull based, i.e., upon request the information is generated and transported towards the sink, compared to other classes where information is pushed towards the sink either periodically or upon some event. The requirement on reliability/latency of query result transport is variable and dependent on the querying application.

Application Requirements on Information Transport

Given the typical WSN applications, we now investigate their requirements on information transport. We identify the following key requirement of ap-

plications on information transport:

Reliability: The conventional requirement of applications for information transport is to receive the information generated in WSN via the sink. The reliability of information transport quantifies the ability of the network to deliver the information. Typically, application requirements are not absolute, i.e., some information loss can be tolerated and are statistical in nature.

Along with reliability of information transport other relevant requirements from applications are:

Timeliness: WSN applications demand the availability of information in time. This can be understood as a requirement on the information transport mechanism to deliver the information as fast as possible (in time).

Energy Efficiency: Application requirement on energy efficiency is directly related with the lifetime of the WSN. Furthermore, the sensor nodes also posses limited energy sources. Therefore, the information transport solution must be energy efficient. Since transmissions are the major factor for energy depletion in WSN, the information transport mechanisms should utilize minimal number of transmissions to deliver the information to the sink.

We assume in this thesis, similar to [Vuran et al., 2004] that the information typically has a temporal and spatial correlation. The information transport strategy should be aware of this fact and accordingly take measures for assuring the reliability of information. The temporal relevance of information is out of the scope of this thesis and we assume that whenever the information is generated it is relevant for the application and should be transported to the sink. In this thesis, we consider the spatial correlation of information and exploit it in order to efficiently transport the information. We also assume that application's timeliness requirement is flexible, i.e., the information remains relevant until it reaches the sink. Despite the fact that we assume flexible timeliness, we show in Chapter 7 that our proposed framework provide low latency compared to state-of-the-art solutions.

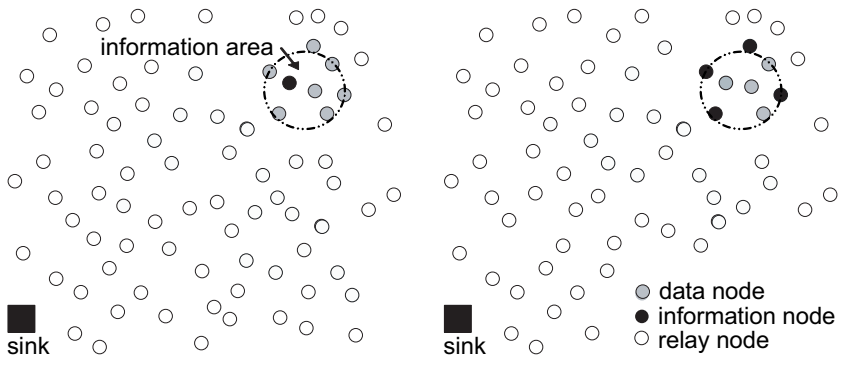
2.3 Information Model

Different applications require different types of information from WSNs. Due to the increasing number of applications running on WSNs, we propose an

abstraction for applications corresponding to the information they expect from a WSN. Such an abstraction supports application independence and transparency for the information transport.

We refer to an *information area* as the geographic area where raw data is generated and the information of interest is extracted through in-network processing as depicted in Figure 2.1. An established example of information area is an event area. The sensor nodes in an information area are classified as *data* and *information nodes*. The data nodes generate raw data while information nodes generate information entities. We refer to an *information entity* as the processed raw data which is required by the application. The data nodes do not send data directly to the sink. On the other hand, information entities generated by information nodes are required to be transported to the sink via relay nodes. In order to achieve tunable reliability of information transport, understanding information is necessary such that different mechanisms can be adapted according to application reliability requirements. Information entities can be generated centrally on a single node (e.g., a cluster head) or in a distributed manner by many nodes (spatially correlated). Information entities can further be grouped/composed for higher semantics and defined as new information, e.g., the event/region perimeter.

Accordingly and without loss of generality we classify any information required by the applications into two broader classes: *Atomic information* and *Composite information*. Atomic information is composed of a single information entity, whereas composite information is composed of more than one information entity as shown in Figure 2.1. Atomic information is complete in nature and cannot be sub-divided, e.g., an aggregated value on a sensor node. On the other hand, composite information is composed from a set of information entities from different sensor nodes (no redundancy). For

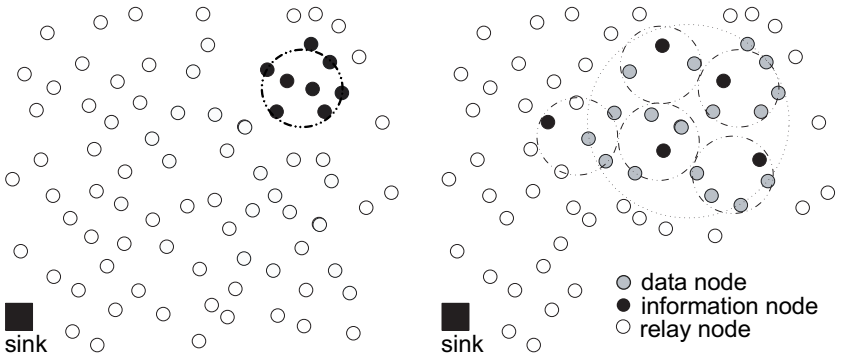


(a) Atomic information (b) Composite information

Figure 2.1: Information classification

example, tracking/event perimeter applications are interested in boundaries of the event/object to better understand its progression. These boundaries can have different shapes/sizes and applications can reconstruct them if they have sufficient information entities, i.e., boundary samples.

We further classify the atomic information into two sub-classes (a) redundant atomic information, and (b) sparse atomic information as shown in Figure 2.2. For redundant atomic information the information generation is dense, i.e., all sensor nodes within the information area generate the respective information entities (Figure 2.2 (a)). For example, in event detection applications multiple sensor nodes detect the event and transport this information towards the sink [Sankarasubramaniam et al., 2003; Zhang et al., 2005]. Sparse atomic information denotes the sparse generation of information, i.e., sensor nodes are unaware of redundant information (Figure 2.2 (b)). For example, due to the clustering factor the event information is generated sparsely at different cluster heads in the information area.



(a) Redundant atomic information

(b) Sparse atomic information

Figure 2.2: Atomic information classification

One of the major issues in order to provide application specific tunable reliability is to select the appropriate sensor nodes for information transport. The purpose of sensor node selection is either to reduce the redundancy of information (redundant and sparse atomic information) or to select an appropriate number of sensor nodes to provide application level fidelity (composite information).

We assume that an information entity is realized through a single message. This assumption is valid, since the majority of the applications require only small payloads to be transported to the sink. Since composite information comprises a set of atomic information, it is easy to transport the composite information by extending the proposed solution of transporting single atomic

information according to application requirements. Furthermore, we consider high information rates, i.e., information bursts to be transported to the sink. In such cases the information has the same properties as discussed above except that the information rate is high.

2.4 Perturbation Model

WSNs are obviously subject to a wide range of computation and communication level faults. Cheap hardware, limited resources and environmental conditions lead to frequent perturbations in WSNs [Arora et al., 2004]. To achieve the desired reliability the proper identification of these perturbations is necessary. Our perturbation model is based on the ability of information transport protocols to tolerate the effects of these perturbations [Walter and Suri, 2003]. We categorize all perturbations encountered during the information transport broadly as intolerable or tolerable perturbations.

Intolerable Perturbations

Intolerable perturbations are those whose effects can not be handled by the information transport framework. WSNs may be deployed in harsh environments such as for fire detection, tracking of people in catastrophic areas. These environments can permanently destroy the sensor nodes on a large scale or the entire WSN, which obviously can not be handled. Other intolerable faults include crash failures of the sink and network partitioning. The sink plays an important role and acts as a bridge between the user and the WSN. Therefore, if the sink crashes, the network will not be able to communicate with the user resulting in an intolerable perturbation. Network partitioning is considered as an intolerable perturbation too, since source nodes and the sink may belong to different network partitions. These intolerable faults can be transformed into tolerable ones, if the maintenance and reconfiguration of the WSN is possible [Gu et al., 2005].

Tolerable Perturbations

Tolerable perturbations are those whose effects can be handled by the information transport framework. We mainly emphasize on the temporal evolvability of the perturbations in WSNs, which hinders in maintaining the required level of application reliability. We classify the tolerable perturbations as communication and node failures.

Communication Failures: Communication failures constitute the most frequent failures in WSNs. Failures relevant to the information trans-

port include message loss, which directly impacts the reliability of the WSN. Collisions and contention constitute the major causes of message loss in WSNs. Collisions occur when two or more sensor nodes transmit messages simultaneously assuming the channel is clear and available for transmission. Once the collision happen, the message is lost. On the other hand, contention refers to situation when the offered load on the link reaches a value close to the capacity of the link. In such a situation, the sensor nodes sense the channel to transmit the messages and find it busy. The sensor node keeps waiting and trying until the channel is clear for transmission. During contention either the sensor nodes after certain attempts discard the messages or they may receive more messages causing buffer overflows leading to message loss.

Node Failures: At node level message loss is caused by congestion and unavailability of sensor nodes. Usually, the congestion is due to increasing network load. When the buffer capacity at a sensor node is exceeded, congestion occurs and results in message loss. The unavailability of sensor nodes can be due to many reasons (1) Sensor nodes usually operate on batteries, which limits the operational lifetime of the sensor nodes. Typically, the drained batteries cannot be recharged or replaced, thus they cannot be part of the network. (2) Sensor nodes are often deployed in harsh environments and may suffer physical damage. (3) Energy saving schemes that are based on duty cycles [Strasser et al., 2007] may be utilized, resulting again in temporary or prolonged sensor unavailability. For the sensor node unavailability, this thesis relies on the underlying routing protocols to provide an alternate good neighbor to route the information.

In order to ensure the desired reliability requirements the framework must overcome these perturbations using both temporal and spatial redundancy techniques for information transport. Temporal redundancy addresses certain actions to be performed over time, e.g., retransmissions to overcome communication failures. Using spatial redundancy, we assume that redundant source nodes or paths are available for information transport towards the sink.

2.5 Reliability Model

The application reliability requirements are generally statistical in nature. For example, monitoring applications do not require reliability of a single information entity but require a certain number of entities to be available over time. Similarly, event detection applications require that a certain number of events to be reported over the lifetime of WSNs. Furthermore, composite information has fine-grained requirements on reliability, i.e., depending on the

shape and size of the phenomenon, the application requirements are changing and may require all the nodes or a subset of them to report. This entails providing x% (probabilistically-guaranteed) reliable information transport instead of best effort or transporting all information entities. Therefore, we define the application reliability as follows:

Definition 2. *The application level end-to-end reliability for information transport R_d ($0 < R_d < 1$) in a WSN is described by the probability of information to be transported successfully to the sink.*

Based on the application requirements, we define atomic and composite information transport reliability as follows:

Definition 3. *The atomic information transport reliability is defined as the degree of tolerating information loss over time.*

Definition 4. *The composite information transport reliability is defined as the degree of tolerating loss of information entities by the application without loosing the semantics of the composite information.*

We transform the application requirement of tolerating $x\%$ false negatives as to provide statistically $(100 - x)\%$ successful transport of atomic information over time. To categorize the reliability of composite information we introduce a $k\text{-}of\text{-}m$ reliability model, where m is the total amount of information entities required and k is desired amount of information entities. Composite information is composed at the sink and $k\text{-}of\text{-}m$ information entities have to be transported by the WSN. We express $x\%$ and $k\text{-}of\text{-}m$ by a probability p with which the WSN transports information entities towards the sink. Consequently, for composite information the framework has to select set of appropriate information nodes.

We assume that the source node knows the reliability with which information is to be transported, i.e., R_d (which takes into account the composition of the composite information or how many times an atomic information entity is replicated). Many existing techniques [Park et al., 2004; Tezcan and Wang, 2007; Wan et al., 2002] can be utilized for a reliable distribution of R_d. Alternatively, the underlying routing protocol can also be used, e.g., through piggy backing to beacon messages. R_d redistribution is only performed if R_d varies.

Chapter 3

State of the Art: Classification, Modeling and Comparison

As an important basis for the context of the research presented in the thesis, this chapter starts by discussing the different data transport semantics in WSNs. Accordingly, the chapter classifies the existing literature and provides analytical reliability modeling basis. Next, based on the classification we survey the state of the art in data transport in WSNs and develop the analytical reliability models for the selected semantics. In last, we compare the existing solutions to get insights and to highlight the drawbacks that hinder the reliability of information transport. The reliability modeling and the comparison of state of the art presented in this chapter constitute one of the key contributions of this thesis, namely **C1** (see Section 1.4.2).

This chapter forms the background and the context for the research questions posed and puts the contributions presented into perspective. The chapter concludes with a discussion on design guidelines for efficient information transport in WSNs.

3.1 Information Transport Semantics

Different number of sensor nodes can be involved for the data generation in the network corresponding to the phenomenon of interest. Consequently, various transport semantics are envisioned for WSNs. In WSNs a prominent semantic used for transport is the *end-to-end (e2e)* data delivery. In e2e semantic, a single sensor node has to transport the data towards the sink. The periodic/continues and some query based applications fall under this category. Another, commonly accepted semantic by the research community is *event-to-end (ev2e)* [Karim et al., 2007; Sankarasubramaniam et al., 2003; Zhang et al., 2005]. This semantic considers multiple sensor nodes reporting the phenomenon of interest to the sink. This semantic is shown to be more suitable than the e2e semantic for WSNs [Sankarasubramaniam et al., 2003]. The ev2e protocols implement a many-to-one process, where the number of relay nodes decreases continuously along the way towards the sink. The ev2e semantic does not require all the data from each sensor node to be available at the sink. The ev2e semantic rely on the fact that for event detection some data can be sacrificed. The e2e semantic is a special case of the ev2e semantic, i.e., where the number of source nodes is one. We also recognize a *hybrid* semantic in WSN, i.e., a fusion of e2e and ev2e semantics. In hybrid solution, each sensor node that detects the event is responsible for sending the data towards the sink.

Generalized Information Transport Semantic: The in-network processing of data is common in WSNs. As soon as the sensed value exceeds a given threshold indicating the existence of the phenomenon, the corresponding sensor nodes generate raw data messages. These messages are disseminated towards the sink. In order to save limited resources such as energy and bandwidth, nodes perform some operations on the raw data and forward the resultant information towards the sink (Figure 3.1). The operations on raw data are primarily filtering, aggregation, information management and routing of the messages. Actually, the information transport starts with the generation of the raw data and comprises the different operations until the phenomenon is reported to the sink.

Hence, complementing the e2e and ev2e, we develop our generalized semantic for data transport:

Definition 1. *Information transport in WSNs is a set of operations carried out on raw data from its generation till the phenomenon is reported to the sink.*

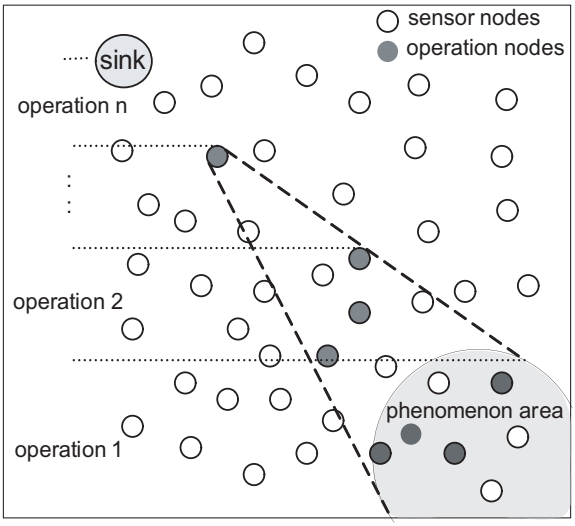


Figure 3.1: Generalized information transport semantic

3.2 Reliability Semantic and Analytical Modeling

As the reliability is a major requirement for information transport, we aim at providing a generic solution that allows for a simple investigation of the information transport reliability. We first define a generic reliability semantic with an appropriate reliability metric. To simplify the computation of this metric, we then provide a reliability model for information transport.

3.2.1 Generalized Reliability Semantic

The reliability of information transport is a function of the reliability of all the operations carried out on raw data. Furthermore, we define the reliability metric as follows:

Definition 2. *The reliability of information transport is the probability that the sink detects the phenomenon of interest within an application specified reliability bound.*

The decomposition of the information transport into operations simplifies the computation of the overall reliability, provided that the dependencies between the reliabilities of the different operations are given. This shows the need for a reliability model that simplifies the calculation of overall reliability of information transport.

3.2.2 Analytical Modeling of Information Transport

Prior to developing the reliability model, we specifically note that our emphasis is on setting up the reliability model for the operational phases of the WSN rather than modifying standardized reliability evaluation schemes.

There are various popular graphical formalisms to express system reliability such as Fault Trees, Markov Models and Reliability Block Diagrams (RBD). We use the RBD approach for its simplicity and its capability of abstracting the system. The reliability of information transport depends on the reliability of each operation performed on the raw data. If one of the operation fails, then the overall information transport fails. According to the RBD theory, this leads to a series representation of the information transport in the WSN. Figure 3.2 depicts the resulting RBD, which outlines the dependencies of the information transport reliability versus the different stages for data operations reliability.

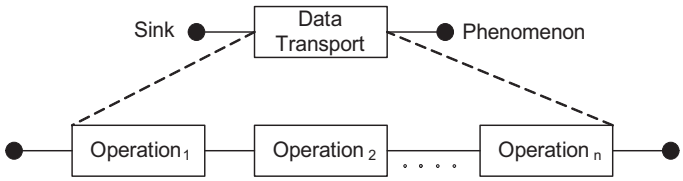


Figure 3.2: RBD for information transport in WSNs

Using Figure 3.2, we calculate the reliability of information transport (R_α) as follows:

$$R_\alpha = R_{op_1} \cdot R_{op_2} \cdot \ldots \cdot R_{op_n}$$

$$R_\alpha = \prod_{i=1}^{n} R_{op_i} \tag{3.1}$$

where R_{op_i} is the reliability of i^{th} operation and $R_\alpha \in [0, 1]$.

Using Equation (3.1), the information transport reliability is calculated provided the number of operations and their reliabilities are known. The reliability of each operation can be calculated either analytically or by simulations. Equation (3.1) assumes that the time specified by the application for information delivery is met by all the operations and the information transport is in-time. The different operations carried out for information transport in turn can be seen as a function of (a) WSN properties and (b) protocol parameters. Unlike the protocol parameters, WSN properties are difficult to control in time. In most of the application scenarios it is difficult to redeploy

the new nodes, or to avoid crashing of nodes due to energy depletion. On the other hand, protocol parameters can be tuned and adapted. The RBD establishes a relationship between WSN properties, protocol parameters and the reliability. Protocol designers can utilize this relationship and implement simple decisions at deployment or runtime. The proposed reliability model can be used to measure and estimate the reliability of information transport in presence of the perturbations. We assume that other operations of information transport are reliable and thus focus on the information transport operation. In order to compare the reliability of existing data transport protocols we investigate the operations performed by the protocols to develop appropriate RBDs.

3.2.3 Ensuring Information Transport Reliability

The major hinderance in ensuring the reliability of information transport is message loss due to various reasons such as environmental inference, contention, congestion, etc. In order to achieve the objective of reliability, the information transport mechanisms have to mitigate message loss and overcome the perturbations, i.e., link losses and congestion. To recover from message loss, generally *retransmissions* are used and for network congestion appropriate *congestion control mechanisms* are deployed.

Message Loss Detection Mechanisms: To enable retransmissions it is necessary to detect the message loss. Several *message loss detection (MLD)* techniques can be adopted by data transport protocols such as Acknowledgment (ACK), Negative ACK (NACK), Implicit ACK (IACK), Explicit ACK (EACK), Selective ACK (SACK), Selective NACK (SNACK) and timers. In WSN hop-by-hop retransmissions are more feasible [Wan et al., 2002] for message loss recovery (MLR). If only the source caches and retransmits the retransmission strategy is termed as *source-to-sink (s2s)*. If the intermediate nodes also cache and retransmit, the strategy is termed as *hop-by-hop (HBH)*. This poses the problem of identifying the cache points (CPs), i.e., where to cache the messages on the way from sources to the sink, either all intermediate nodes on the path or a subset of them should cache.

To overcome message loss, apart from retransmissions, multipath and forward error codes (FEC) can also be utilized. In multipath strategies, message is sent on several paths concurrently towards the sink. Multipath solutions exploit path redundancy in order to reduce the chances of message loss. Using FEC the sensor node sends more data than the original generated data in order to overcome the partial message losses, such that the original data can be reconstructed at the sink.

Congestion Control Mechanisms: Congestion control comprises of

schemes to detect the congestion and alternatively avoid or mitigate it. Upon congestion detection (CD), sensor nodes trigger congestion notification (CN) by disseminating the appropriate indicator to the relay and the source nodes. The source nodes realize congestion mitigation (CM) by dynamically adjusting their data rate. The common approach for the data rate adjustment is Additive-Increase and Multiplicative-Decrease (AIMD) [Sankarasubramaniam et al., 2003; Wan et al., 2003]. Some approaches propose to conduct the adjustment in a discriminative manner depending on the fidelity of the source nodes such as exact rate adaptation (ERA) or start/stop rate adaptation (SSRA).

3.3 Categorization and Modeling of Existing Solutions

Based on the given background and discussion, we now present the state of the art for different data transport semantics (Figure 3.3) and provide reliability modeling.

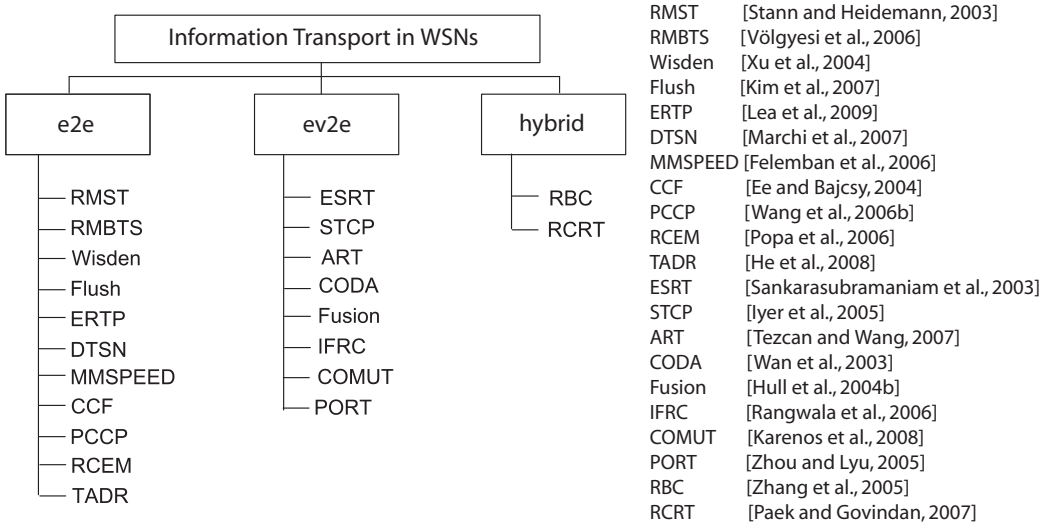


Figure 3.3: Classification of data transport protocols

3.3.1 The e2e Class

The main objective of the literature in this class is to assure and maximize the end-to-end reliability of data transport. Table 3.1 compares the different

strategies for e2e data transport in WSNs. We first review the major protocols in this class. Subsequently, we consider the abstraction for e2e and provide RBD modeling for calculating reliability.

	Reliability		**Congestion**	
	MLD	**MLR**	**CD**	**CM**
RMST	SNACK	HBH/s2s	x	x
RMBTS	NACK	s2s	x	x
Wisden	NACK	HBH/s2s	x	x
Flush	SNACK	s2s	x	x
ERTP	IACK	HBH	x	x
DTSN	ACK/NACK	HBH	x	x
MMSPEED	x	multipath	x	x
CCF	x	x	buffer+MST	ERA
PCCP	x	x	MAT+MST	AIMD
RCEM	x	x	buffer	multipath/AIMD
TADR	x	x	buffer	multipath

Table 3.1: Strategies for e2e semantic

Reliable Multi-Segment Transport (RMST) [Stann and Heidemann, 2003] protocol provides data transport reliability and is built over Directed Diffusion [Intanagonwiwat et al., 2003] routing protocol. The reliability in RMST refers to the eventual transport of all messages from the sensor nodes to the sink. RMST is a SNACK and timer driven protocol and places responsibility for MLD at the receivers (which can be intermediate nodes as well as the sink). The missing message requests are explicitly sent as a uni-cast from the sink towards the source node. RMST has two working modes, i.e., the non-caching mode and the caching mode. In the non-caching mode, only the sink and the source node are involved in the loss detection and s2s recovery is carried out. On the other hand, in-network caching allows fast recovery such that the lost messages can be recovered from intermediate nodes in HBH manner. The major drawback of RMST is that it is tightly coupled to Directed Diffusion routing protocol [Intanagonwiwat et al., 2003]. Furthermore, RMST requires each intermediate node to cache all the messages received from sources, which makes the scalability of RMST doubtful. RMST is only suitable for the applications that require large size data, to take advantage of fragmentation at the source and reassembly at the sink. Moreover, RMST might not be suitable for reliably delivering data from multiple source nodes, since they cause more contention for the channel.

Völgyesi et al. in [Völgyesi et al., 2006] proposed the Reliable Multihop

bulk Transfer Service (RMBTS). The protocol uses NACK based s2s message recovery scheme for lost messages. The sensor nodes update their next hop for forwarding the data based on the reliability scores gathered by continues monitoring of the path. The sensor nodes utilize Request-to-Send (RTS) and Clear-to-Send (CTS) control schemes to allocate channel for sending messages between the neighbor nodes. In RMBTS source nodes are responsible for caching the data and MLR is initiated by the sink. The s2s recovery of messages is not feasible in WSN, since it requires a lot of transmissions for recovery compared to HBH scheme. Furthermore, RTS/CTS schemes also require control messages to be exchanged which result in further transmissions.

Xu et al. presented Wisden [Xu et al., 2004], a structural data transport system. Wisden periodically collects structural response data for monitoring damages. Wisden provides reliable data transport by using a hybrid message recovery scheme, i.e., HBH and s2s. Wisden uses hop-by-hop NACK scheme, where each source node stores the data in its EEPROM and then transmits to the neighbor node towards the sink. The sensor nodes keep a small cache of recent messages, from where the lost messages are recovered. Furthermore, Wisden also uses an s2s NACK based scheme for MLR. When a sink detects the message loss, it propagates the request for missing messages toward the source node. Since the source node maintains the generated messages in its EEPROM, it retransmits the missing messages. Wisden is similar to the scheme proposed in RMST.

Kim et al. proposed Flush [Kim et al., 2007], for bulk data transferring from a source node to a sink. Flush utilizes a sink to coordinate data transport and uses s2s based SNACK for MLD. First, Flush queries the topology to compute the Round Trip Time (RTT) for timeout estimation at the sink. The sink uses RTT to decide when to send a request for lost messages. Second, the source sends messages to the sink at the maximum rate by avoiding intra-path interference. Third, the sink sends the sequence numbers of the lost messages back to the source using NACK. After receiving NACK, the source retransmits the missing messages. This process continues until the sink receives all the requested lost messages. In last, the sink verifies the integrity of the data. If the integrity check fails, the sink will discard the data and initiates a fresh request.

In [Lea et al., 2009], authors have proposed energy efficient and reliable data transport protocol (ERTP) for WSNs. ERTP uses IACK as MLD. The retransmissions are dynamically calculated and carried out in HBH fashion to recover message losses. ERTP proposes a distributed mechanism for calculating retransmission timeouts to control unnecessary retransmissions. ERTP also incorporates message duplication detection and suppression in order to

avoid same messages to be transported many times. The messages are stored at the intermediate sensor nodes until IACK is received.

Distributed Transport for Sensor Networks (DTSN) [Marchi et al., 2007] utilizes s2s retransmissions and FEC to enhance the reliability. DTSN supports differentiated reliability, i.e., total and partial reliability. The total reliability is based on s2s Selective Automatic Repeat Request (ARQ) with caching at intermediate sensor nodes. DTSN also utilizes ACK or NACK depending on the existence of gaps in the received messages at the sensor node. The partial reliability is achieved by employing the Enhancement Flow and FEC mechanisms. The Enhancement Flow option provides a fraction of data to be buffered at the source (called as the core) for transmitting with total reliability. The remaining data is forwarded with no guarantees, since they are considered as the enhancement data. Generally, FEC requires a high computation thus limiting the practicality of DTSN for WSNs.

In [Felemban et al., 2006], the MMSPEED protocol is proposed for probabilistic QoS guarantees in WSNs supported by multipath forwarding. MMSPEED forward messages according to their specific reliability and timeliness requirements. For the timeliness MMSPEED provides multiple speed options to forward and meet the end-to-end deadlines of the messages. To achieve reliability MMSPEED uses probabilistic multi-path delivery. MMSPEED controls the number of paths depending on the required reliability. MMSPEED assumes that eventually the data will be received by the sink over multiple paths and thus does not store the data on source as well as on intermediate nodes. The majority of multipath approaches [Caleffi et al., 2008; Deb et al., 2003b; Hsu et al., 2007; Kulik et al., 1999; Lee and Gerla, 2001; Teo et al., 2008] utilize multiple paths from the source node to the sink in order to load balance the network. On the contrary, the multipath protocols are required to maintain the multiple paths which are not efficient and use more transmissions resulting in limiting the overall lifetime of the network.

Ee et al. [Ee and Bajcsy, 2004] presents congestion control and fairness (CCF) scheme for data transport in WSNs. CCF utilizes local congestion detection based on buffer occupancy and message service time (MST). The proposed rate control scheme is based on HBH implicit back-pressure mechanism. When the sensor node's buffer is threshold full it sends the back-pressure message to its upstream neighbors to reduce the data rate. When the buffer becomes empty the node starts transferring the data at higher rate. More specifically, CCF involves following steps: First, the sensor nodes measure the average data rate by estimating the inverse of the time required to transmit a message using an exponential moving average. Second, based on the total number of child nodes CCF assigns appropriate data rate to them. When the sensor node encounters congestion it assigns reduced data

rate to its children. Third, CCF compares the data rate of the parent and its children and disseminates the smallest rate to the child nodes. The CCF's fairness scheme uses probabilistic or epoch based selection of sensor nodes for sending their data.

Priority based Congestion Control Protocol (PCCP) [Wang et al., 2007a] calculates a congestion degree as the ratio of message arrival time (MAT) and MST. PCCP uses ERA for data rate adjustment. PCCP allocates priority to the sensor nodes based on application requirements and the node with higher priority gets higher bandwidth. PCCP maintains different priorities for forwarded and generated messages. PCCP uses implicit CN by piggy backing the header of the forwarded messages, thus avoiding additional control messages and mitigating LL congestion efficiently.

In [Popa et al., 2006], to increase throughput of e2e data transport, a location based protocol is designed for WSNs called as RCEM. The RCEM approach consists of a multipath routing protocol based on Biased Geographical Routing (BGR), and two congestion control algorithms, In-Network Packet Scatter (IPS) and End-to-End Packet Scatter (EPS). BGR forwards the messages on curved trajectories instead of shortest path towards the sink. IPS is utilized to overcome SL congestion by splitting traffic before the congested areas. On the other hand, to alleviate LL congestion EPS is utilized by splitting the flow at the source and adapting the data rate. The sensor nodes explicitly send messages for CN such that IPS and EPS can be triggered.

Authors in [He et al., 2008] present a solution for SL congestion by utilizing the idle or under loaded sensor nodes and propose a traffic aware dynamic routing (TADR) algorithm. TADR routes messages around the congested areas and split the flow along multiple paths. TADR uses the concept of potentials in physics, by constructing a mixed potential field of energy depth and normalized buffer length. The obtained potential field forces the messages to overcome the obstacles (congestion) and move towards the sink. The congestion is detected by using buffer occupancy and explicitly communicated to the neighbor nodes. TADR is designed for SL congestion and assumes that the source nodes cannot adapt data rate.

The e2e Reliability Modeling

Revisiting Table 3.1 reveals that e2e protocols either provide reliability or congestion control. The basic technique to increase the reliability of e2e data transport is retransmission. These protocols differ mainly in the policies for adapting MLD. Each method proposes a strategy to detect message loss and allocate the nodes that can retransmit lost messages and perform the congestion control. Modeling the reliability of these protocols is therefore

similar. For this reason we utilize a generic abstraction to model the e2e semantic.

Operations on data transport from the source to the sink in e2e semantic are divided as follows:

Routing: This operation is used to identify potential routes for transporting the generated messages.

MLD: MLD is an essential operation for reliable data delivery. MLD is used for retransmission of missing data. Also, MLD is used to detect message losses due to congestion.

For reliable delivery of e2e, missing data is detected by using appropriate MLD as discussed in Section 3.2.3 and retransmitted. The failure of one retransmission does not result in the failure of complete data transport. This effect is shown as parallel RBD blocks for e2e in Figure 3.4. The gray block represents the operations not considered by the protocols and provide flexibility to include other operations when needed.

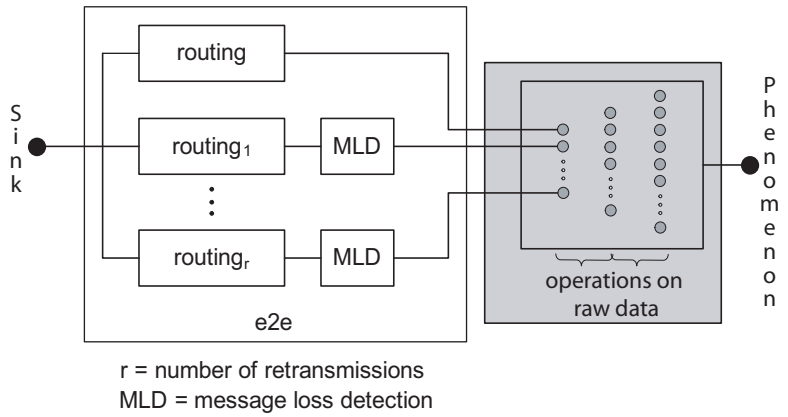


Figure 3.4: RBD for e2e semantic

The number of retransmissions plays an important role in the reliability of the data transport. The designer can use this model to determine the expected number of retransmissions to achieve the desired reliability.

Using Figure 3.4, the reliability of e2e (R_{e2e}) is calculated as follows:

$$R_{e2e} = 1 - \{(1 - R_R) * (1 - (R_R * R_{MLD}))^r\} \tag{3.2}$$

where R_R is the routing reliability and R_{MLD} the reliability of MLD.

R_R and R_{MLD} vary with respect to the protocols used, the environment where the WSN is deployed and the network conditions.

3.3.2 The ev2e Class

Several ev2e protocols have been proposed for data transport in WSNs as shown in Table 3.2.

	Reliability		**Congestion**	
	MLD	**MLR**	**CD**	**CM**
ESRT	#msg received	x	buffer	ADR
STCP	NACK/ACK	s2s	buffer	AIMD
ART	NACK/ACK	s2s	ACK loss	SSRA
CODA	x	x	buffer+channel	AIMD
Fusion	x	x	buffer	SSRA
IFRC	x	x	buffer	AIMD
COMUT	x	x	buffer (cluster level)	AIMD
PORT	x	x	channel	ERA

Table 3.2: Strategies for ev2e semantic

Event to Sink Reliable Transport (ESRT) [Sankarasubramaniam et al., 2003] achieves the reliability objective by adjusting the data rate of source nodes by avoiding congestion. In ESRT, the sink adjusts the data rate of the source nodes according to the network state, i.e., network congestion. ESRT assumes that the sink requires certain number of messages for an event within application specified time interval. The message loss is only due to the congestion. At the end of a time interval, the sink makes a decision based on number of messages received and the congestion state of the network. ESRT does not utilize retransmissions to recover message loss and relies on the fact that at least some messages from source nodes will arrive at the sink, as all messages contain the same information. The sensor nodes detect the congestion by observing the buffer occupancy. If the sensor node's buffer is threshold full the node specifies congestion bit in the forwarded messages. When the sink receives fewer messages along with congestion bit enabled it will request the source nodes to decrease the data rate. ESRT is not energy efficient, since the data rate is controlled centrally. Furthermore, ESRT assumes that the sink can reach and communicate with all source nodes directly, which is not a reasonable assumption in practical WSN deployments. Also, as the network state dynamically changes, the central congestion mitigation decisions are not feasible. To regulate the congestion ESRT changes the data rate of all sensor nodes, which is also not practical because different sensor nodes contribute towards different levels of congestion.

Yogesh et al. proposed a Sensor Transmission Control Protocol (STCP) [Iyer et al., 2005] for WSNs. STCP provides variable reliability, congestion

control and supports s2s and ev2e data flows in the network. Before sending the data the sensor nodes establish session with the sink. During session establishment the sensor node informs the sink about the number and type of flows, the data rate and the reliability requirement. The sink stores this information, initiates proper parameters and sends ACK message back to the sensor nodes. For s2s data flow, end-to-end NACK is utilized. If the sink does not receive the data from the sensor nodes within estimated time, it will send a NACK. The time estimation for STCP requires clock synchronization between the sink and the source nodes. Upon receiving the NACK sensor nodes retransmit the missing messages. On the other hand, s2s ACK is used for the ev2e data flows. The source nodes store the data until they receive the ACK from the sink. The source nodes also utilize timers during which if the source node does not receive ACK it assumes that the message is lost and retransmits the message. STCP detects congestion based on the buffer length. STCP maintains two thresholds for each sensor node to monitor congestion. When the buffer reaches the first threshold, the congestion bit is set with a certain probability. Whereas, when the buffer reaches the second threshold, all the messages contain the congestion notification. When the sink receives messages with congestion bit enabled, it informs the source nodes about congestion via ACK. After receiving the ACK informing about congestion notification, the source nodes either route the remaining messages along different paths or modify the data rate. STCP is also not energy-efficient as the data rate is controlled centrally. Furthermore, STCP requires clock synchronization for all the sensor nodes in the network, which may result in poor performance. Also, ACK from the sink for ev2e data flows may result in high latency in large scale WSNs.

Asymmetric Reliable Transport (ART) [Tezcan and Wang, 2007] provides reliability of data from the sensor nodes to the sink and vice versa. ART divides the network into essential and normal sensor nodes. The essential nodes are the set of sensor nodes having more energy and cover the entire sensor field using a weighted greedy algorithm. ART utilizes timer driven retransmissions between essential nodes and source nodes. For event transport, ACK mechanism is used while NACK strategy is used for reliable query delivery. ART also includes a distributed congestion control mechanism, where congestion is alleviated by regulating data from non essential sensor nodes. To regulate congestion ART utilizes SSRA scheme. When ACK is not received by the essential nodes, they request that the non essential nodes to stop sending their data. Once the essential node starts receiving the ACK again, it asks the non essential nodes to report their data. The congestion detection by ACK loss is not an efficient solution, since ACK can also be lost. As the essential nodes are only responsible for reliability and conges-

tion control, the message from non essential nodes will go un-noticed and their recovery is not guaranteed by ART.

In [Wan et al., 2003] the authors have developed a congestion control strategy for WSNs called as Congestion Detection and Avoidance (CODA). CODA has three components: congestion detection, open-loop hop-by-hop back-pressure and closed-loop end-to-end multi-source regulation. CODA attempts to detect congestion by monitoring current buffer occupancy and wireless channel load. CODA periodically samples the channel load and compares it with the theoretical channel utilization to detect congestion. Furthermore, if the buffer occupancy is beyond a pre-defined threshold the sensor node perceives the congestion. Once the congestion is detected, the sensor node explicitly broadcasts a suppression message to notify its neighbors and makes local adjustments to prevent congestion propagation. When messages are forwarded during congestion, the sensor nodes include regulation bit in the messages to notify the sink about the congestion. In the closed-loop multi-source regulation mechanism the sink is responsible for the congestion control. When the sink receives messages with the regulate bit set, it sends ACKs to regulate the source nodes. When ACK is received by the source sensor nodes, they reduce the sending rate according to some rate decrease function (e.g., multiplicative decrease). CODA's congestion detection mechanism is reactive in nature which leads to the dropping of messages. CODA shows poor congestion control as the number of source nodes and data rate increases. Furthermore, the closed-loop multi-source regulation increases the latency under LL congestion.

Fusion [Hull et al., 2004b] provides fairness guarantees among source nodes along with congestion mitigation by utilizing prioritized MAC. Fusion uses HBH back-pressure mechanism for rate control and utilizes local congestion detection approach. When the buffer utilization is high, i.e., if the buffer is threshold full, the sensor nodes detect congestion and insert congestion bit in the forwarding messages. For HBH flow control Fusion uses an implicit mechanism where sensor nodes snoop the messages to check the congestion bit. If the congestion bit is set the sensor nodes throttle their data rate to alleviate the congested state. To limit the data rate at sensor nodes a passive snoop-based approach is used such that the data rate of child and parent sensor nodes will be same. In the case of congestion, the parent node generally has more traffic to forward than the child nodes. Thus, in order to provide more access to parent node, Fusion proposes a prioritized MAC technique. The backoff timing for a node is a function of sensor node's local congestion state and number of its child nodes. The congestion aware backoff interval increases the chances of congested sensor to gain access of the wireless channel. In addition, the prioritized MAC also provides fairness

by giving priority to intermediate traffic over source traffic.

Interference Aware Fair Rate Control (IFRC) [Rangwala et al., 2006] proposes interference aware congestion control mechanism. IFRC uses local congestion detection based on the monitoring of the buffer occupancy. In IFRC the sensor node allocates and controls the data rate of its upstream and interfering neighbor nodes. IFRC considers all the links which create interference. If a node starts sending the data towards the sink and mark them as potential interferers. Thus, for many-to-one data delivery, a set of potential interferers of a node include its neighbors, neighbors of its parent and as well as neighbors of its parent's parent. In detail, IFRC is composed of three components (1) congestion detection, (2) congestion circulation and (3) rate adaptation. IFRC uses exponentially weighted moving average of buffer occupancy for congestion detection. IFRC utilizes two thresholds for inferring congestion at the sensor node. When congestion is detected IFRC reduces the data rate to half. When congestion is alleviated, IFRC increases the data rate additively. IFRC circulates the congestion and data rate state among the neighbors to ensure the fairness for data delivery. The IFRC's goal is to assign the data rate which is lowest among the interfering neighbors of the congested node. The rate adaptation of the source nodes in IFRC is based on AIMD scheme.

Kyriakos et al. in [Karenos et al., 2008] presents a cluster based congestion control scheme for multi-class data flows called COMUT. COMUT ensures that flows with the higher importance will be dealt appropriately in order to provide higher fidelity and timeliness than the flows with lower importance. COMUT locally detects the congestion based on the node's current buffer occupancy. COMUT's rate control algorithm is centralized and run at the cluster head. Essentially, each sensor node reports its local congestion state to the cluster head. In turn, the cluster heads periodically exchange the aggregated congestion level and importance of the data flow among other cluster heads along the path towards the sink. The cluster head proactively monitors and predicts the congestion in localized manner. In order to estimate the traffic intensity and data rate adaptation the cluster head calculates a collective estimate of load for the cluster by using the local readings from each cluster member. To detect congestion at the cluster level a threshold value is applied (calculated analytically). COMUT rate adaptation policy is also based on AIMD. However, for less important data flow COMUT drops the data rate to some minimum rate.

Zhou et al. proposed a Price-Oriented Reliable Transport protocol (PORT) [Zhou and Lyu, 2005]. PORT aims to provide fidelity of interested events while minimizing energy consumption. PORT proposes a price mechanism to measure the communication cost from a sensor node to the sink.

The node price is defined as the total number of transmissions from a source to a sink for achieving successful message delivery. To ensure the fidelity of the collected events, PORT estimates the optimal application level reporting rate based on the node price. To improve the data reliability each node dynamically allocates its outgoing traffic based on the neighboring node's prices. PORT also employs a mechanism for controlling the data rate of the source node based on its price. The end-to-end data rate adjustment mechanism provides reliability of interested events while minimizing energy consumption.

The ev2e Reliability Modeling

The task of the existing ev2e transport protocols is to report the events of interest to the sink. In ev2e, each node that detects the phenomenon sends the data towards the sink. If the data from one source node is not delivered, the application can tolerate this and data transport will not fail. Therefore, according to the RBD theory data transport for ev2e consists of n parallel routing blocks as shown in Figure 3.5.

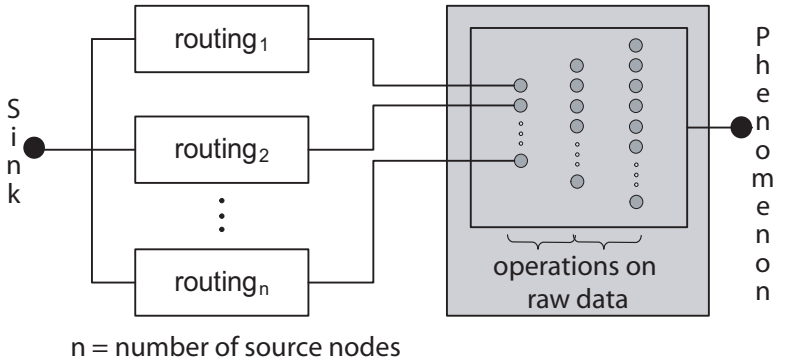


Figure 3.5: RBD for ev2e semantic

We calculate the reliability of ev2e (R_{ev2e}) as follows:

$$R_{ev2e} = 1 - (1 - R_R)^n \tag{3.3}$$

where R_R is the routing reliability and n is the number of sources reporting the phenomenon to the sink.

3.3.3 The Hybrid Class

There are very few works considering hybrid data transport semantic as depicted in Table 3.3.

	Reliability		Congestion	
	MLD	**MLR**	**CD**	**CM**
RBC	Block ACK/IACK	HBH	x	x
RCRT	NACK	s2s	RTT	ADR

Table 3.3: Strategies for hybrid semantic

Reliable Bursty Convergecast (RBC) protocol [Zhang et al., 2005] is designed for transferring a burst of messages from the source nodes to a sink. The RBC reliability design is based on a window-less block ACK and IACK scheme that enables continuous message forwarding in the presence of message and acknowledgment loss. The sensor node organizes its buffer as a number of linked lists called virtual queues based on number of maximum retransmission. Each virtual queue buffers messages waiting to be sent or to be acknowledged. The RBC protocol provides message reliability through HBH retransmission based loss recovery where intermediate nodes cache the messages. RBC proposes intra- and inter-node message scheduling to avoid collisions. To improve channel utilization, RBC introduces differentiated contention control, which ranks nodes according to their buffering conditions and the number of transmitted messages. Moreover, to improve the network throughput, RBC allows new messages to be sent out without waiting for ACK of the previously sent messages. RBC aims at transporting messages to a sink with 100% reliability. The virtual queuing mechanism adapted by RBC is not memory efficient and requires more memory for memory constrained sensor nodes.

In [Paek and Govindan, 2007] a centralized rate controlled reliable transport protocol (RCRT) is presented for WSNs. RCRT is composed of s2s retransmission, congestion detection, data rate adaptation and data rate allocation mechanism. Each source node stores a copy of the message to recover message loss using NACK. The sink keeps track of sequence numbers of messages it receives and when a gap in sequence number is detected, NACK with missing messages is sent towards the source node. RCRT decides about the congestion by observing the behavior of message losses across the network, i.e., if message losses require more time to recover than the estimated time the congestion is assumed in the network. The time to recover message loss is set as the multiple of RTTs. Once the congestion is detected by RCRT, it estimates the total sustainable traffic in the network and allocates the data rate to the data flow. Conversely, if congestion is not detected RCRT additively increases the data rate for each flow. RCRT focuses on achieving 100% reliability by overcoming congestion without consideration of energy-efficiency

and tunable reliability.

The Hybrid Reliability Modeling

In hybrid semantic all the source nodes send data towards the sink and loss of data is not tolerable. Thus, it can be viewed as a special case of e2e where instead of single source node, a set of nodes are transmitting the data using e2e semantic. This results in parallel combination of e2e blocks. The resultant RBD for the hybrid semantic is shown in Figure 3.6.

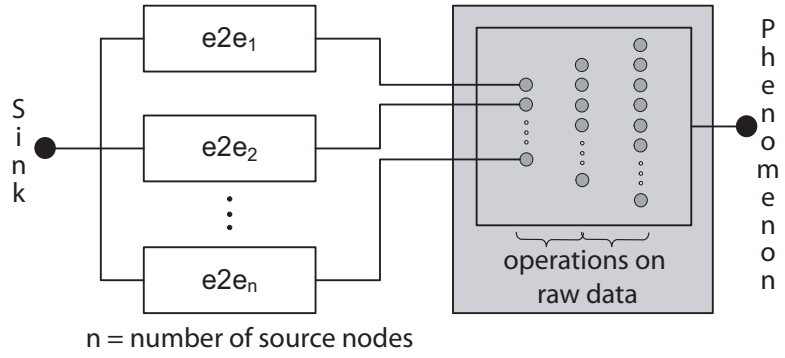


Figure 3.6: RBD for hybrid semantic

Accordingly, the reliability of hybrid semantic (R_{hybrid}) is calculated as follows:

$$R_{hybrid} = 1 - (1 - R_{e2e})^n \tag{3.4}$$

where R_{e2e} is the reliability of the e2e scheme and n is the number of sources reporting the phenomenon to the sink.

Substituting Equation (3.2) in Equation (3.4) we obtain,

$$R_{hybrid} = 1 - (1 - \Big[1 - \{(1 - R_R) * (1 - (R_R * R_{MLD}))^r\}\Big])^n \tag{3.5}$$

3.3.4 Analysis of Reliability Modeling

After computing the reliabilities for different data transport semantics, we explore how perturbations and important protocol design parameters impact these reliabilities. We investigate the impact of the retransmission strategy and especially the number of retransmissions on the reliability of the e2e protocols. For the ev2e and hybrid protocols, we compare their reliability corresponding to the number of source nodes.

Figure 3.7 shows the impact of the number of retransmissions on the reliability of e2e using Equation (3.2). We investigated the number of retransmissions by fixing the routing and MLD reliability at different levels. Our purpose of tuning the reliability levels is to model the behavior of perturbations. In the case of high routing and MLD reliabilities we observe that after two retransmissions the reliability remains close to 1.0 and the impact of further retransmissions on the reliability is minimal. In case of low routing and high MLD reliability, after eight retransmissions the reliability of e2e becomes close to 1.0. In all scenarios after a certain number of retransmissions the behavior remains same and the retransmissions become useless and waste limited resources. These results are in agreement with the results in [Zhao and Govindan, 2003]. However our study specifically provides a new approach to easily determine the number of retransmissions needed for a given MLD strategy and a given routing reliability.

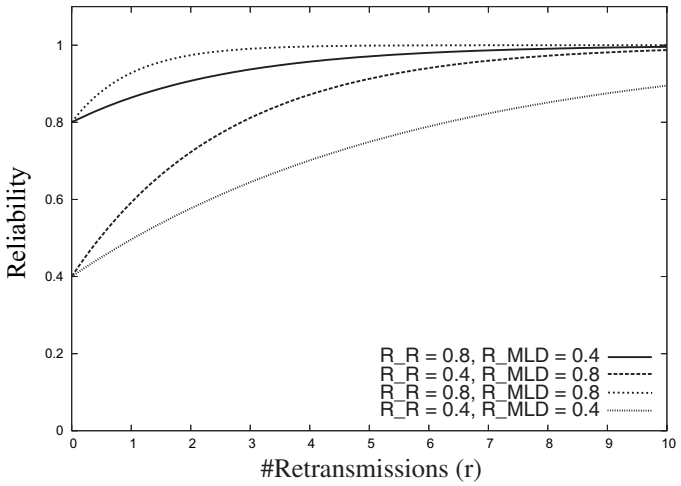


Figure 3.7: Impact of number of retransmissions on e2e reliability

Figure 3.8 plots the reliabilities of ev2e and hybrid (using Equation (3.3) - (3.4)) for different number of sources and different failure rates. We have fixed the number of retransmissions in hybrid equal to three similar to [Zhao and Govindan, 2003]. Also we have fixed the reliability of MLD as 0.8. We observe that if routing reliability is high, then we require less number of sources for reporting the phenomenon. In this case ev2e and hybrid performed equally good due to the fact that at a higher routing reliability, less retransmissions are needed. For a routing reliability of 0.5 hybrid requires two reporting nodes, whereas ev2e requires six reporting nodes to achieve a reliability close to 1.0. This signifies that hybrid requires fewer nodes to send data to the sink, saving precious resources in the network. For routing reliability less

than 0.5 we require higher number of sources.

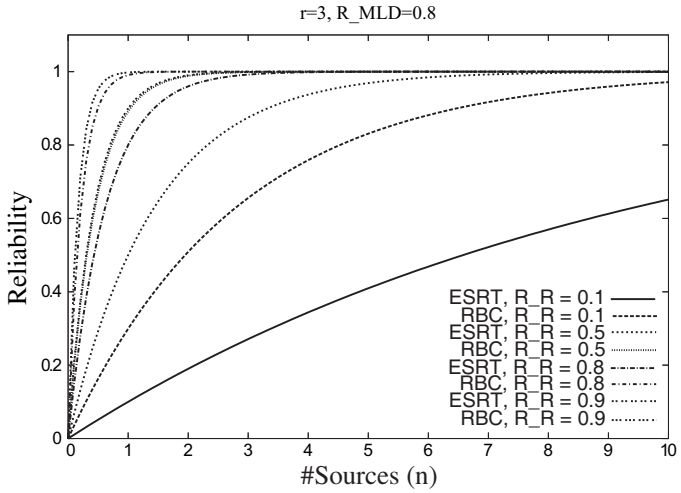


Figure 3.8: Comparison of the reliability of ev2e and hybrid

Online Adaptation for Data Transport Reliability

Our proposed modeling technique can be easily utilized for online adaptation of protocols by tuning the protocol parameters according to current network conditions. Assuming that at time t_o application requirements for delivery reliability R_o are available to protocol, e.g., sink disseminates the application requirements to the sensor nodes. Also the current network properties at t_o are available to the sensor nodes, e.g., via routing layer, facilitating the protocol to compute its parameters. As shown in Figure 3.9, considering e2e for instance, R_{R_o} and R_{MLD_o} reflect the current network conditions. The sensor nodes can keep track of network conditions either locally or sink can disseminate this information. Consequently, the protocol parameter r_o can be computed by using inverse function of Equation (3.2) as follows:

$$r_o = \frac{log(1 - R_o/1 - R_{R_o})}{log(1 - (R_{R_o} * R_{MLD_o}))} \tag{3.6}$$

If R_R or R_{MLD} varies over time, r will be tuned appropriately such that the required degree of reliability is maintained. Similarly if the application varies its requirement for delivery reliability, r will be tuned to attain the level required by application.

Now we compare the representative protocols from each category comprehensively via simulations and show their behavior for evolving network conditions.

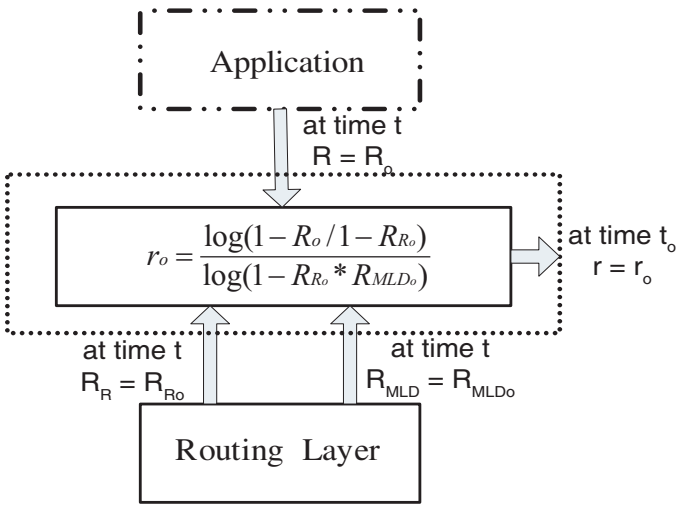


Figure 3.9: Online adaptation for e2e

3.4 Comparison of Existing Solutions

In order to compare the existing data transport protocols we first select the representative protocols then describe our methodology and simulation settings. Next, we classify the scenarios into five main studies to cover a wide representative range of network operational conditions and protocol parameters.

Most existing e2e data transport protocols address retransmission and congestion control separately (Table 3.1). For congestion control a detailed analysis is presented in [Vuran et al., 2005], therefore in comparative study we mainly focus on retransmissions strategy. As discussed earlier, e2e protocols are similar in nature and differ only in the approaches for MLD, CP, CD and CM techniques. Therefore, instead of focusing on different e2e protocols we consider a skeleton (SKE) protocol comprising hop-by-hop retransmission strategy, which is the most efficient [Stann and Heidemann, 2003; Wan et al., 2002] with CP at all intermediate nodes. Generally, the ev2e protocols implement many-to-one process. Some ev2e protocols only tackle congestion where as few deal with both reliability and congestion. We select ESRT as a representative protocol for ev2e due to its popularity and since it is one of the first solutions which provide the notion of ev2e semantic. For hybrid class we identify only two protocols, i.e., RBC and RCRT. As RCRT's major functionality is at the sink, which is not much suitable for WSNs, we chose RBC as a representative protocol for hybrid class.

3.4.1 Experimental Environment

TinyOS 1.1.15 [TinyOS, 1999] is an open-source operating system designed for WSNs. The TinyOS architecture is composed of components, which enables rapid development with minimal code size as required by inherent memory constraints of sensor nodes.

TinyOS's simulator, called TOSSIM [Levis et al., 2003], is a discrete event simulator intended for simulating homogeneous sensor networks. In TOSSIM each sensor node runs the same program. The user can compile TinyOS applications for TOSSIM and run them on a PC instead of sensor nodes.

TOSSIM allows users to debug, test, and analyze the algorithms in a controlled and repeatable environment. TOSSIM's main goal is to provide a high fidelity simulation of TinyOS applications. It simulates WSN at the bit level and captures every interrupt in the system.

TOSSIM provides abstractions of certain real-world phenomena (such as bit errors). With tools outside the simulation environment, users can then manipulate the abstractions to implement other real world models. TOSSIM does not model the radio propagation, instead it provides a radio abstraction using directed independent bit errors between two sensor nodes. The desired radio model maps its behavior to the bit errors. The directed independent error bits relate to the fact that asymmetric links can be easily modeled and the message loss probability is independent.

Although TOSSIM captures TinyOS behavior at a very low level, it makes several simplifying assumptions. Therefore, it is possible that the code which runs in a simulation might not run on a real sensor node.

We now define the metrics upon which the framework will be evaluated.

3.4.2 Performance Metrics

The performance of the techniques is measured in terms of responsiveness and efficiency. The responsiveness of the information transport is regarded as reliability and timeliness, whereas the efficiency is mainly given by the message complexity.

Information Transport Reliability: The information transport reliability is the relative amount of the information received by the sink compared to the total amount of information generated.

Timeliness: Timeliness is defined as the time elapsed from the generation of the first information entity to the arrival of the first information entity at the sink. The timeliness of the framework is the average information transport latency of all generated information entities. As some information entities may not be reported at the sink, we do not consider the corresponding

entities in the calculation of the average information transport latency.

Efficiency: As the efficiency is measured in terms of message complexity, we define the message complexity as the total number of message transmissions required for the information transport (including the retransmissions). We note here that communication between nodes is regarded as the highest energy consuming factor. Therefore, this metric can be utilized to estimate the energy efficiency of the framework.

3.4.3 Methodology

To compare the data transport protocols the underlying network stack protocols are also considered.

MAC Protocol considerations: For MAC the major distinction is between the use of TDMA or CSMA to resolve channel access. We focus on CSMA-based implementations, because, although several TDMA protocols have been proposed [Coleri-Ergen and Varaiya, 2006; Rajendran et al., 2003], their implementation in TOSSIM is not available. Under CSMA-based implementations BMAC [Polastre et al., 2004] and SMAC [Ye et al., 2004a] are widely used MAC protocols [Malesci and Madden, 2006] for TinyOS. Only BMAC implementation is available in TOSSIM for simulation. Therefore, we had to limit ourselves to BMAC [Polastre et al., 2004]. The MAC layer does not perform any retransmissions, but notifies the routing layer above of missing acknowledgements for uni-cast traffic.

Routing Protocol considerations: Fundamentally, there are two major classes of routing, i.e., *reactive* and *proactive* [Al-Karaki and Kamal, 2004]. Reactive protocols find the route only when there is data to be transported. Proactive protocols on the other hand, find paths in advance and periodically exchange topology information to maintain them. In literature there are several proactive routing protocols [Al-Karaki and Kamal, 2004]. For routing the messages, RBC uses by default Logical Grid Routing (LGR) [Choi et al., 2004] protocol. Since LGR is the representative proactive routing protocol, we have chosen LGR for routing the messages for proactive class. For, the reactive class we have chosen TinyAODV [TinyAODV, 2003] because it is the only available reactive protocol in TinyOS repository and also it is a ZigBee standard routing protocol. The code of RBC is available for the mica2 mote platform, consequently we ported the RBC code to run under the TOSSIM environment. Since, the code for e2e protocols and ESRT is not available, we implement SKE and ESRT in TOSSIM. We extracted the retransmission strategy from RBC [Zhang et al., 2005] and used it as a basis for the SKE protocol.

The topology that we used in our simulations consists of typically used

n x n grid topology. The distance between the two nodes is denoted as the *cell size*. The sink is available at the upper left corner. In case of ESRT and RBC protocols, s sensor nodes from each of the remaining three corners of the grid, that are geographically close to each other, generate an event message to be transported to the sink as shown in Figure 3.10. For SKE which is a representative e2e protocol, one node is sending data to the sink. We assume some local signalling as a complementary to SKE such that instead of s sensor nodes, a single node from each corner send event information.

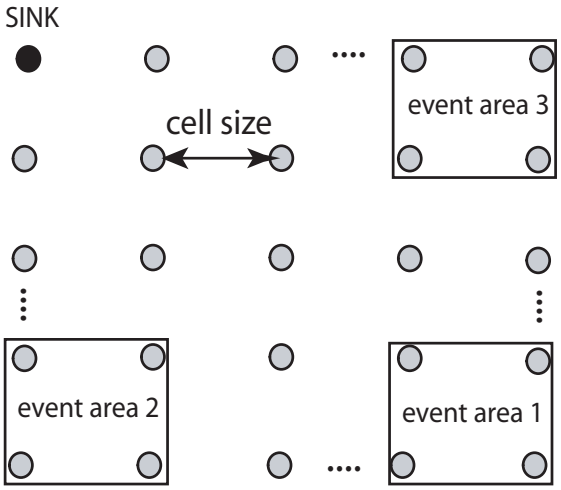


Figure 3.10: Scenario settings

In our experiments three events are generated simultaneously to be transported towards the sink. Two protocol parameters are of primary concern for data transport protocols, i.e., number of sources s and number of maximum retransmissions r. In this work we assume $s = 4$ for ESRT and RBC protocols, whereas for SKE $s = 1$. RBC uses $r = 3$ by default and to enable a conformal comparison between e2e and ev2e protocols, we set the maximum number of retransmission for the SKE protocol equal to the number of sources of ESRT and RBC, i.e., $r = 4$. An event message is generated after 40 sec from the start of the simulation to give enough time for the network to stabilize. We assume that an event can be reported as a single message and if the sink receives at least one event message, the event is considered to be detected.

3.4.4 Description of Comparative Studies

We measured the values of the above described metrics depending on the network properties, routing protocols and protocol parameters. We base

our comparison on the five studies. In each study, we investigate the impact of relevant network property on the responsiveness and efficiency of the SKE, ESRT and RBC protocols. The considered network properties include number of nodes, network connectivity and bit error probabilities (BEP). Furthermore, we tune the most relevant protocol parameters and suggest adaptation issues for these parameters. Unless specified, we have used LGR as underlying routing protocol.

Study 1: Impact of Network Scale: The purpose of this study is to investigate the ability of the protocols to maintain the responsiveness and efficiency as the number of nodes varies. Scalability is always a concern for protocol designers and this study enables us to observe the scalability of protocols. Furthermore, varying the number of nodes reflects the different operational situations occurring in WSN, e.g., node crash, re-deployment of nodes and duty cycling. In [Woo et al., 2003] the authors have shown that nodes having a maximum communication range of 50 units, have good connectivity between them only when they are 7.5 unit apart. Nodes having distances over 7.5 unit experience transient connectivity. For this study we set the *(cell size)* to 7.5 unit, to have relatively good communication between the neighbors.

Study 2: Impact of Network Connectivity: The main objective of this study is to show the robustness of the protocols to network connectivity changes. For this study we change the network connectivity by varying cell sizes from 2.5 to 20 unit. As we increase the cell size, a node has limited connectivity to its neighbors.

Study 3: Impact of Bit Error Probability: The objective of this study is to show the robustness of the protocols to varying link qualities. This is crucial for WSNs as the link quality may change during the lifetime of the application. We consider the wireless channel BEP, which varies the link reliability. In wireless communication, sometimes high average BEP from 10^{-4} to 10^{-2} is possible [Karl and Willig, 2005]. In this work we vary the BEP between a node and its neighbors from 0 to 10^{-3}, reflecting a wide range of cases. This study also covers the scenarios, where the network is congested. Collisions and congestion leads to corruption of packets, which is similar to corruptions of bits.

Study 4: Impact of Routing Protocols: Existing data transport protocols assume the existence of a routing protocol. Designers in general evaluate their protocols for their favorite routing protocol. In a recent comparative study [Malesci and Madden, 2006], the authors showed that there is no routing protocol that outperforms all others in all network conditions. Therefore, a deeper analysis of the impact of routing protocols on the performance of data transport protocols is of a great interest. In this study we investigate

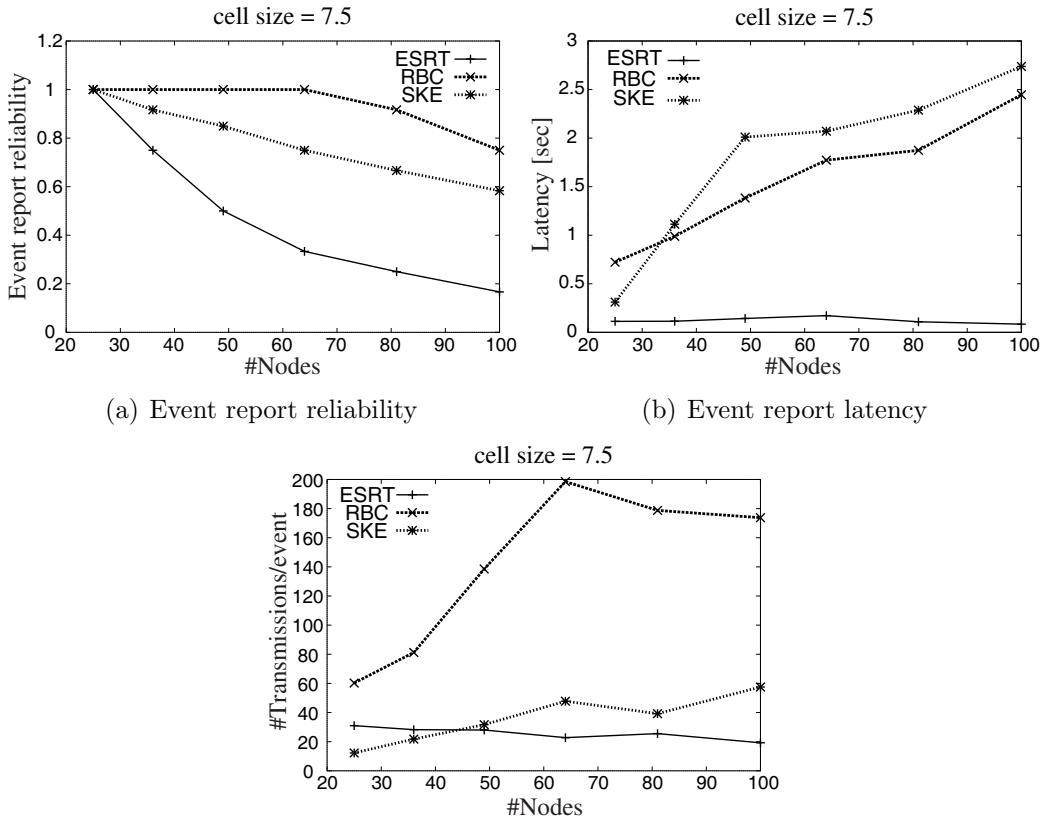
the impact of reactive routing protocols on responsiveness and efficiency of data transport protocols and compare it with proactive routing protocols.
Study 5: Tuning data transport Protocol Parameters: We investigate the impact of tuning data transport protocol parameters for responsiveness and efficiency. For this study we take RBC as the reference protocol and tune parameters for ESRT and SKE. RBC uses $s = 4$ and $r = 3$, so in the worst case altogether 12 retransmissions takes place for each event. Accordingly, we tune for the SKE protocol ($r = 12$) to have the same maximum number of transmissions for a single event. It should be noted that for SKE we can not tune s, as for SKE only one source is available. We term this tuned SKE protocol as SKE-3x. To increase the reliability of event reporting the authors of ESRT [Sankarasubramaniam et al., 2003] suggest to increase the data rate. Therefore, for ESRT we kept $s = 4$ and increased the data rate to 3 messages per event per source instead of 1 event message per source. We term this version of ESRT as ESRT-3x. The approach here is to investigate which protocol parameters are suitable to achieve higher event report reliability. Either we increase the data rate for an event or we increase the maximum number of retransmissions to achieve higher event report reliability.

3.4.5 Comparison Results

In this section we discuss the results of simulations that were conducted for the selected protocols.

Impact of Network Scale

Figure 3.11 (a) displays the observed event report reliability for each of the selected protocols for different number of sensor nodes (from 5x5 to 10x10 grid topologies) while fixing the cell size to 7.5 unit. We examine that as the number of nodes increases, the event report reliability tends to decrease and none of the protocols shows 100% event report reliability. This is due to the fact that the number of hops are increased between source nodes and the sink. However, RBC's event report reliability remains always higher than ESRT and SKE. The event report reliability of ESRT is decreasing gradually as the number of nodes increases because ESRT is not retransmitting the lost packets. With increase in number of hops the probability of packet loss increases, thus reliability decreases with the number of hops. Similarly, the event report reliability of SKE and RBC also decreases gradually with network scale. Figure 3.11 (b) shows that with an increase in number of nodes, the latency is also increased. This is also expected as with the increase of number of nodes, the number of hops also increases between source nodes and the sink,



(a) Event report reliability

(b) Event report latency

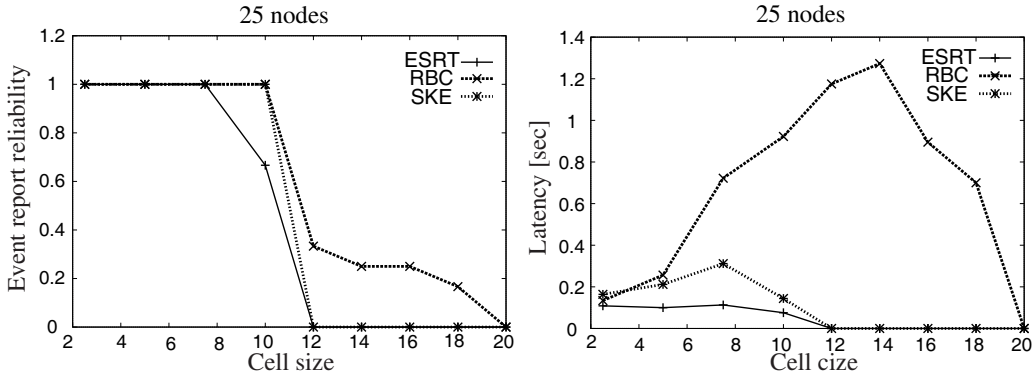
(c) Event report efficiency

Figure 3.11: Impact of network scale

thus the event messages are passing through more nodes. This behavior is specific to the underlying routing protocol that chooses nodes's parent in the spanning tree based on number of hops. In this way a message takes more time to reach the sink. ESRT's latency always remain low which is directly related to low event repot reliability. On the other hand, SKE's latency is in most cases highest corresponding to the fact of low number of sources reporting an event and reliability is reached by successive retransmissions. RBC uses the highest number of transmissions compared to ESRT and SKE as shown in Figure 3.11 (c). For RBC, the number of transmissions tends to increase as the number of nodes increases since more intermediate nodes are retransmitting the event messages. For SKE the number of transmissions are less for fewer number of nodes and as the number of nodes increases, SKE's number of transmissions increases owing the increase to the number of hops. ESRT shows lower number of transmissions that corresponds to the fact of decrease in event report reliability.

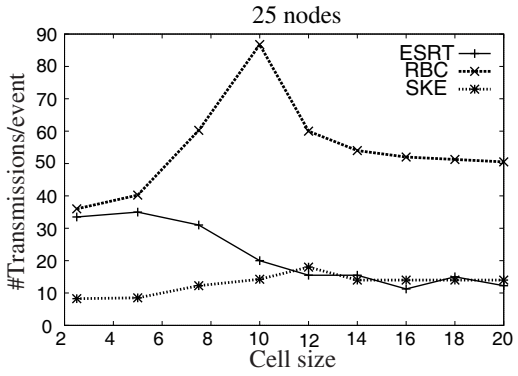
Impact of Network Connectivity

Figure 3.12 shows the event report reliability, latency and efficiency for 25 nodes at different cell sizes. Figure 3.12 (a) shows the RBC protocol is performing better than ESRT and SKE with respect to event report reliability owing to the use of retransmissions and ACK mechanisms. When the nodes have good connectivity all three protocols are showing high event report reliability. We also observe that as the network connectivity decreases the event report reliability also decreases. RBC is always more resilient than ESRT and SKE. The SKE protocol is performing well compared to ESRT, owing to the HBH retransmission strategy. Whereas for ESRT, once a message is lost, it is lost forever. In all cases we observe that beyond a cell size of 10 unit the protocols are not performing well with respect to event report reliability, suggesting that these protocols are not suitable for networks to be deployed in lower network connectivity. From Figure 3.12 (b) we conclude that the latency of the ESRT is the lowest. The latency values should be



(a) Event report reliability

(b) Event report latency



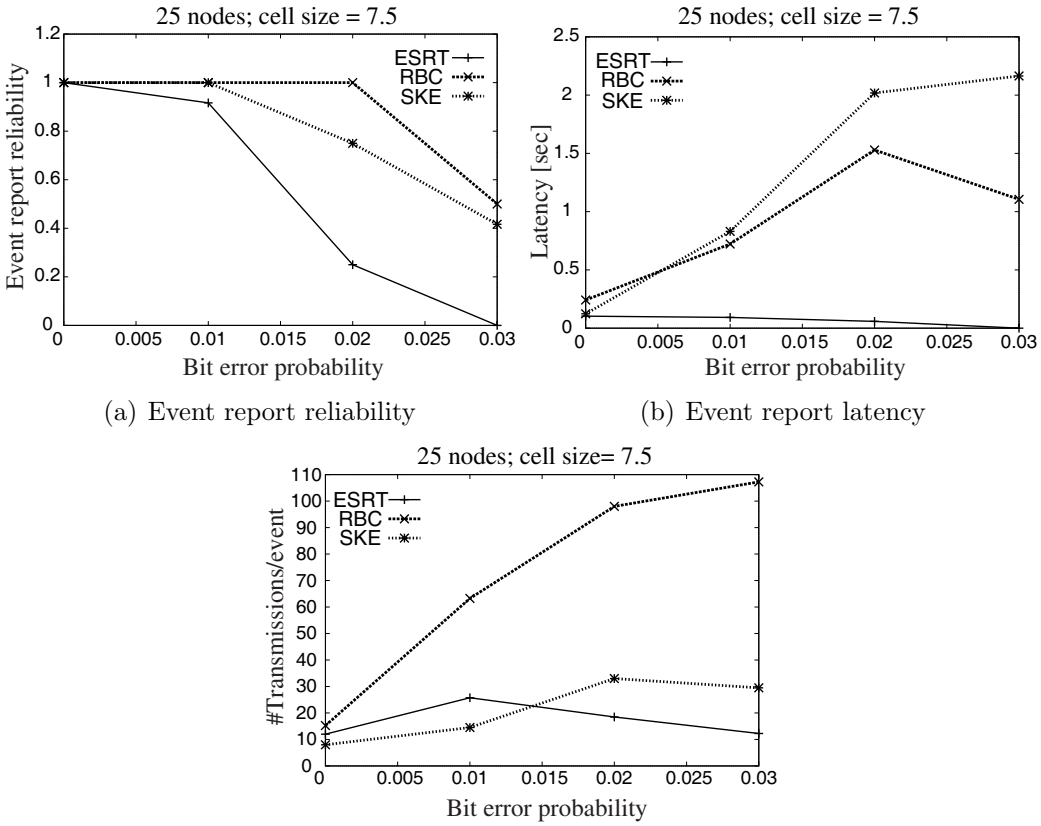
(c) Event report efficiency

Figure 3.12: Impact of network connectivity

interpreted together with the event report reliability. RBC and SKE show higher latencies since they retransmit the message at intermediate hops. The latency of SKE is relatively lower than that of RBC, as SKE has fewer event reporting sources. In general, as the network connectivity decreases the latency of RBC and SKE increase due to the fact that both protocols have to retransmit the messages more times, to be reported to the sink. The latency of RBC and SKE start decreasing as network connectivity is getting worse because the number of successfully reported events is lower. As expected the number of transmissions for RBC is always higher than ESRT and SKE as shown in Figure 3.12 (c) especially for large cell sizes. We observe that for higher network connectivity SKE is more efficient, but as the network connectivity decreases, the number of retransmissions slightly increases as the nodes have limited connectivity with their neighbors. We also observe that as network connectivity starts to decrease, the number of transmissions increases for RBC because all nodes along the path are retransmitting to achieve higher event report reliability. Beyond cell size of 10 unit the number of good neighbors decreases and thus the reliability of route towards the sink becomes lower, resulting in less number of transmissions for RBC. Similar effect is observed for ESRT and SKE as well.

Impact of Bit Error Probability

Figure 3.13 (a) shows that as BEP is increased, the event report reliability is decreased. For lower bit error probabilities, all protocols perform equally well. SKE and RBC perform well at high bit error rates compared to ESRT. This suggests that these protocols perform well in erroneous conditions with collisions and high contention, and shows their robustness against these problems. At lower BEP the latency of ESRT is low (Figure 3.13 (b)) out-performing SKE and RBC because ESRT does not implement a retransmission mechanism. This shows that at lower BEP the overhead of retransmission can be avoided. We observe that at a higher BEP the latency of SKE is much higher than that of RBC owing to the lower number of sources. In general as the BEP increases, the latencies of SKE and RBC increase. Figure 3.13 (c) shows that the efficiency of RBC decreases at high BEP, but this is the cost of its high event report reliability. At low BEP, SKE is more efficient owing to the fact that one node is sending the event information. With increasing BEP the number of transmissions also increases to maintain higher event report reliability. For ESRT, at lower BEP the number of transmissions slightly increases and as BEP increases the number of transmissions decreases, since at higher BEP ESRT is unable to forward the messages.



(a) Event report reliability

(b) Event report latency

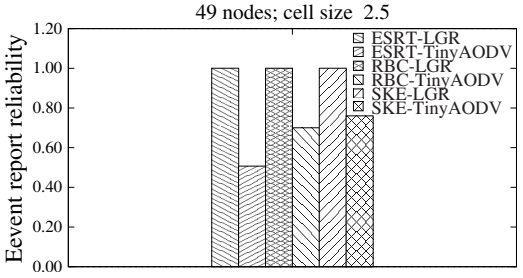
(c) Event report efficiency

Figure 3.13: Impact of bit error probability

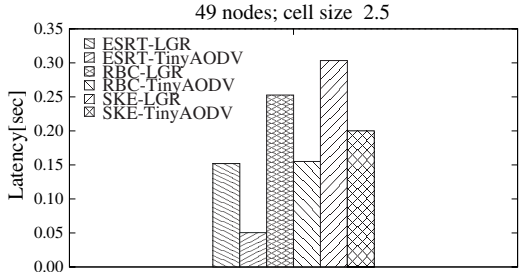
Impact of Routing Protocols

Figure 3.14 (a) shows the impact of changing the routing protocol on event report reliability for 49 nodes and cell size of 2.5 unit. We observe that using LGR the event report reliability of all data transport protocols is 1 whereas the use of TinyAODV provides the event report reliability between 0.5 to 0.75. This is due to the fact that TinyAODV uses flooding for route discovery, and for some nodes either route request (RREQ) or route reply (RREP) messages are lost because of collisions. Therefore, these nodes could not establish a route to the sink. We also noticed that the event report reliability was high when a route was in the local cache of a node. This suggests that the routing success rate is driven by the efficacy of route establishment. Since, routes are established via flooding, the higher the number of sources trying to establish routes, the lower the likelihood of a route to be established successfully. Subsequently, the event report reliability of SKE is higher than

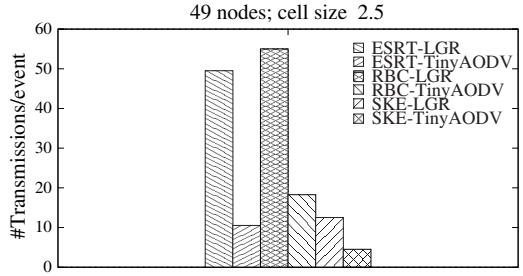
that of other data transport protocols when using TinyAODV suggesting that the reactive protocols are not suitable for event driven applications where simultaneously more nodes are sending event information towards the sink. Figure 3.14 (b) and Figure 3.14 (c) show the latency and efficiency



(a) Event report reliability



(b) Event report latency



(c) Event report efficiency

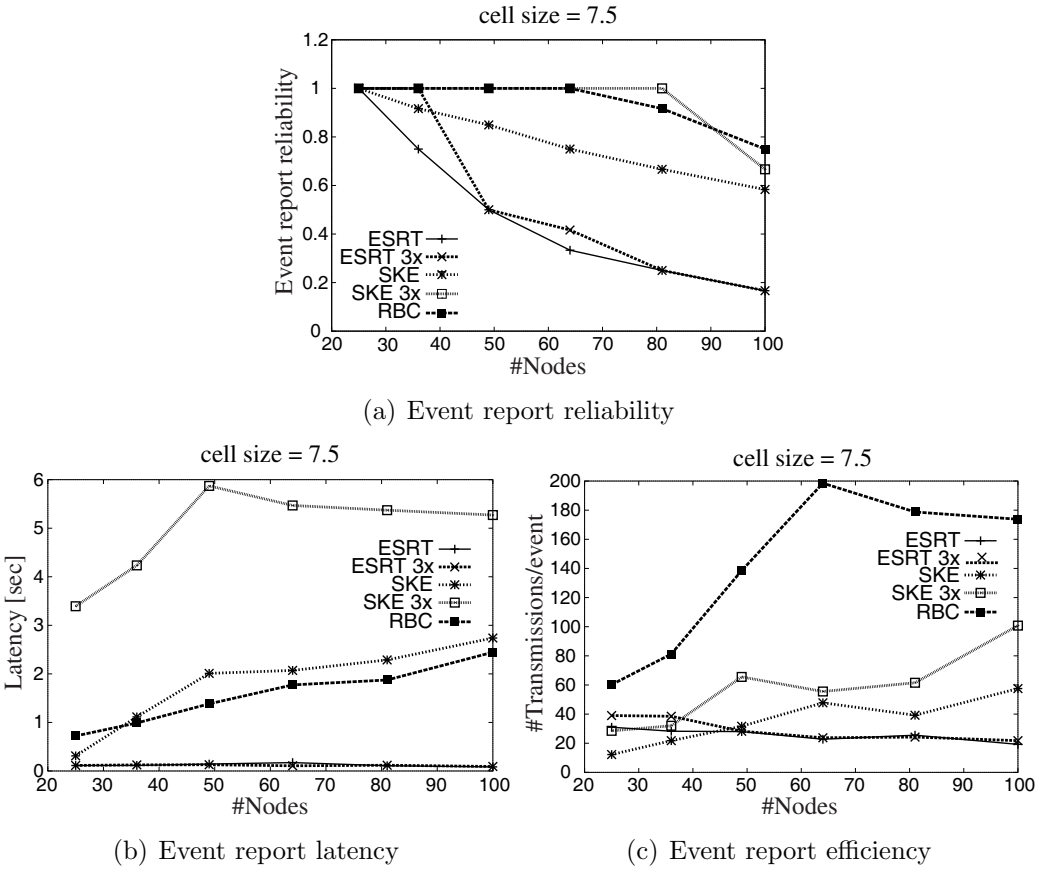
Figure 3.14: Impact of routing protocols

of data transport protocols for different routing protocols respectively. We notice that latency and efficiency of TinyAODV are lower compared to LGR which correlates with its lower event report reliability. Furthermore, the latency and efficiency are related with the route length and the quality of its links. We observe that TinyAODV selects the forwarding node from which it gets RREP irrespective of its link reliability and thus the route is shorter and has less reliable links. LGR takes care of quality of links by periodic beaconing and selecting more reliable neighbors to forward the data

which leads to longer route. This results in more transmissions and increased latency for LGR, but higher event report reliability. If an initially found route is unreliable TinyAODV generate new RREQ which further degrades the performance of data transport protocols.

Tuning Data Transport Protocol Parameters

Now we investigate the impact of tuning the protocol parameters on the responsiveness and efficiency. Figure 3.15 (a) shows that by allowing SKE-3x to retransmit more, the event report reliability is increased significantly. Whereas ESRT-3x, while sending more messages, does not achieve higher event report reliability. It should be noted that for fewer number of nodes, ESRT-3x also shows improvement and achieve higher event report reliability compared to ESRT. By tuning SKE-3x ($r = 12$), it is comparable to RBC for higher number of nodes, as it can retransmit more often. This shows the



(a) Event report reliability

(b) Event report latency

(c) Event report efficiency

Figure 3.15: Impact of tuning data transport protocol parameters

usefulness of adaptation of protocol parameters. Figure 3.15 (b) shows that SKE-3x has the highest latency. This is obvious due to the fact that the event messages are retransmitted and almost never lost. However, this is a tradeoff between reliability and timeliness. This also shows that (1) in worst case scenarios, when only one node is able to detect the event, the event is reported to the sink (2) for delay tolerant applications such mechanisms are beneficial. The latency of ESRT-3x is similar to ESRT and very low, making it efficient, but less reliable compared to other protocols. Figure 3.15 (c) depicts the efficiency of the protocols. We observe that the RBC has a higher number of transmissions in comparison to all other protocols. One important observation about SKE-3x is that it uses comparatively fewer transmissions, as it is using one source node. Furthermore, it suggests that SKE-3x requires fewer retransmissions to achieve high event report reliability and is more efficient than RBC. This also shows that tuning $r = 12$ is more optimistic and SKE-3x achieves event report reliability with relatively lower number of retransmissions. This study suggests that the protocol parameters are important for the performance of any data transport protocol and should be tuned carefully to achieve high responsiveness.

3.5 Chapter Summary

This chapter presented the context of the reliability of data transport problem that this thesis intends to solve, alongside with a survey, modeling and comparison of the state of the art in the field of WSNs.

Our simulation study has quantified the certainty of the textual statement of the existing data transport protocols surveys [Akyildiz et al., 2002; Wang et al., 2006c; Willig and Karl, 2005] and showed new behaviors as we simulated a wide range of scenarios.

In the light of our experimental analysis, we observe that the protocols behave differently for a given application scenario and show different tradeoffs between reliability, timeliness and efficiency (Table 3.4). For example, hybrid protocols provide more event report reliability and timeliness but exhibit poor efficiency. The ev2e protocols provide good timeliness and efficiency but perform poorly for event report reliability. On the other hand e2e protocols perform well with respect to event report reliability and efficiency but their timeliness is poor. Overall the hybrid protocols perform better than the e2e and ev2e protocols in terms of event report reliability and timeliness. For small scale networks and for scenarios where BEP is lower, e2e protocols outperform other approaches with respect to both efficiency and event report reliability. We also observed that existing protocols can not be deployed in

harsh environments where network connectivity is transient or volatile.

	hybrid	ev2e	e2e
reliability	+	−	+
timeliness	+	+	−
efficiency	−	+	+

Table 3.4: Comparison of data transport protocols

Our study shows that data transport protocols have to cope with the dynamic and evolvable network properties. Therefore, adaptation of data transport protocol parameters is needed. The number of retransmissions and number of sources per event are clearly the two adaptation criteria which can be tuned, depending on the length and reliability of the route towards the sink. This is also evident from our proposed reliability modeling. Additionally, from this study it is evident that the link quality, quantified by BEP is a suitable indicator to trigger an online adaptation process. Capturing the BEP of the link (or level of congestion) at runtime and then setting the optimal number of retransmission is very promising adaptation.

The lack of an integrated approach that provides tunable reliability for information transport combined with congestion control and information management in WSNs motivated us to design a generalized application specific information transport framework. Furthermore, recent surveys [Rahman et al., 2008; Wang et al., 2006a] also emphasize the need for such an integrated solution.

Chapter 4

Generic Information Transport Framework for WSNs

The evolving application requirements and dynamic network conditions complicates the design of a generic solution for information transport in WSNs. This chapter targets a comprehensive solution for information transport in WSNs and accordingly proposes a Generic Information Transport (GIT) framework. Our approach is to design an adaptable solution which provides necessary tools to support generalized applications based on abstract system, perturbation, information and reliability models. GIT manages the information and utilizes a probabilistic approach to ensure tunable reliability of information transport. GIT conducts its functionality in a decentralized manner. The proposed modular architecture keeps the generality of GIT intact by allowing different modules to adapt/reuse existing mechanisms.

In particular, this chapter makes the following contributions.

- We design the GIT framework to provide tunable reliability of information transport for various information types despite evolving network conditions.
- We develop a modular architecture in order to seamlessly integrate and tune the building blocks of GIT.
- We develop mechanisms to efficiently consider the properties of the information of interest (type and level of redundancy), while providing fully tunable reliability of information transport.
- We adapt appropriate techniques in order to allow a localized/efficient and on-the-fly tunability of reliability. In next chapters we elaborate the techniques adopted by GIT in a comprehensive manner.

In Chapter 7, the simulation results validate the tunability of the GIT framework. In some setups GIT achieves up to 4-5 times reduction in number of transmissions compared to existing approaches.

The proposed GIT framework constitute the major contribution (**C2**) of the thesis and provide the answers to the raised research questions in Section 1.4.1. Next, the design objectives and requirements by GIT framework are described. Subsequently, the proposed GIT framework is presented followed by different modules of GIT. Finally, the contributions of the chapter are summarized.

4.1 Design Objectives and Requirements

In the following we discuss the design considerations for information transport framework in WSNs. First, we outline the design objectives that should be followed by the information transport framework to cope with the distinct properties of WSNs. Then, we argue for the basic requirements to achieve the stated design objectives.

We believe that tunability, decentralization, adaptation, scalability, perturbations tolerance and resource-awareness are the key design issues for WSN applications in general and for information transport in particular.

Tunability: Due to varying, evolving and statistical nature of reliability requirements by WSN applications, a framework should be able to ensure tunable reliability of information transport. The different mechanisms should adapt and tune in order to fulfill the desired reliability requirements.

Decentralization: Conventionally, a sink is utilized to centrally manage the different operations of the WSN at the cost of huge overhead of communication. With the evolving network conditions the central role of the sink becomes more inefficient. Therefore, efficient decentralized or localized mechanisms should be developed for the framework.

Adaptation: Due to the diversity of WSN applications and the continuously evolving network conditions, a generalized solution that is applicable for most (and ideally for all) network and application scenarios is needed. Thus, online adaptation to the key WSN characteristics should be considered towards the development of the framework.

Scalability: Generally, WSNs are envisioned for large scale deployments. Accordingly, the framework should scale in terms of number of nodes efficiently without excessive overhead and should provide simple mechanisms for resource constrained sensor nodes to reliably transport the information.

Fault Tolerance: The failures are norm rather than the exception in WSNs. Thus, the framework should deal with disruptions and unpredictable network conditions.

Resource Efficiency: The framework and its mechanisms are supposed to run on sensor nodes with limited energy, computational power and memory. Consequently, the mechanisms should be frugal by design and resource efficient.

For a generic information transport framework we derive the basic design requirements based on the application requirements, WSN characteristics and the presented design objectives. We distinguish the following design requirements on a generalized framework for information transport in WSNs.

- The framework has to deal with generic characteristics of WSNs and diversified applications. Therefore, it is required that the framework should be realized keeping in view the limited sensor node capabilities and should be as general as possible.
- The sensor node selection is an essential requirement for information transport, since selecting more sensor nodes having the same information corresponds to more transmissions in the network.
- Maximizing efficiency is a major requirement of WSNs due to limited energy resources. Therefore, the framework has to reduce number of messages as much as possible. The message complexity is also a good indicator of energy consumption, bandwidth utilization and the storage overhead.
- As the global state in WSNs is hard to obtain, another requirement on generic framework is that nodes adapt to local network parameters independently. This means that each node should be capable of tuning the parameters of the framework based on its local perspective on the network.

4.2 The Proposed Framework

Considering the generalized WSN models discussed in Chapter 2, we now present a generic solution that dynamically and autonomously adapts to maintain the desired information transport reliability. First, we provide a conceptual overview of GIT framework. Next, we show how it adaptively integrates and controls temporal and spatial redundancy techniques on-the-fly to provide tunable reliability of information transport.

4.2.1 Overview: The Modular Approach

In order to appropriately tune the reliability of information transport it is necessary to (1) manage different types of information and their level of redundancy, (2) cope with perturbations, and (3) select and tune the suitable reliability assurance techniques. To fulfill these objectives GIT proposes four modules that reside on each sensor node as shown in Figure 4.1.

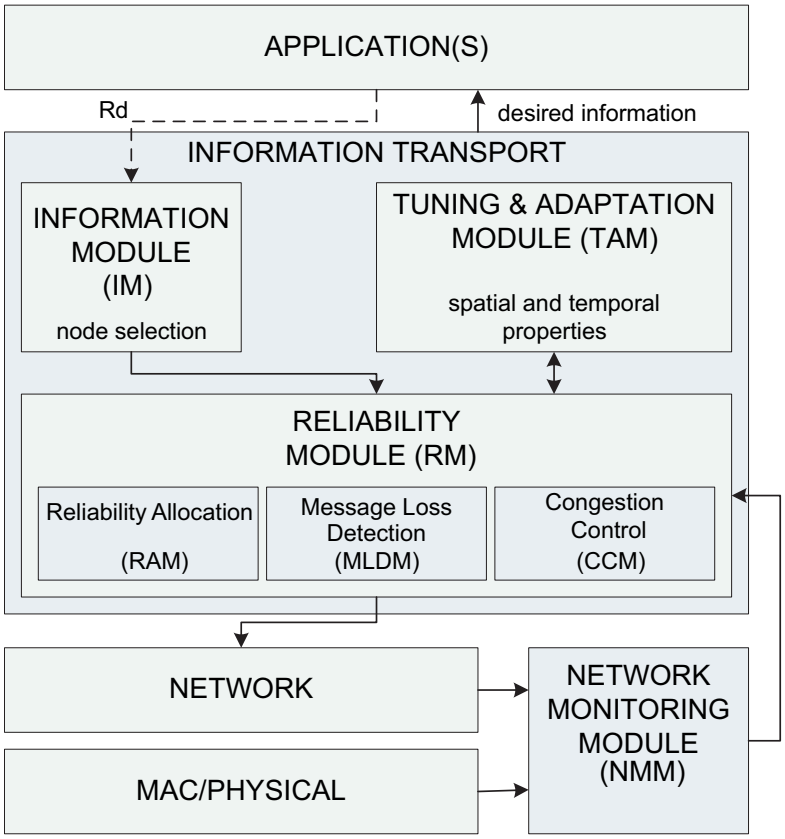


Figure 4.1: The GIT framework

The modular approach allows for the easy integration of different mechanisms with GIT modules. Once the information of interest is generated inside the network the information module (IM) identifies and removes redundancies from the information before transporting it to the sink. We develop efficient and distributed techniques for information management that are utilized by IM (Section 4.3). In Chapter 5, we show that how spatial correlation of information can be exploited in order to achieve and maintain the tunable reliability of information transport. In WSNs (given the power depletions of the sensor nodes and the lossy nature of their communications) perturbations are the norm rather than the exception which hinders in the delivery of information to the applications. To handle perturbations GIT provides a reliability module (RM), which incorporates multiple techniques to locally detect information loss. The wireless medium and limited memory capabilities of the sensor nodes are major causes for information loss. To appropriately detect these losses, GIT integrates a message loss detection module (MLDM) and congestion control module (CCM). In WSNs

information often has to travel multiple hops to reach the sink. To maintain application reliability along the entire path, RM also includes a reliability allocation module (RAM) which allocates reliability across the hops. To recover information loss, GIT provides a tuning and adaptation module (TAM). TAM exploits existing approaches for utilizing in-network spatio-temporal redundancies to overcome the information loss. The subsequent chapters (Chapter 5 and Chapter 6) provide a basis for RM and TAM modules of GIT framework. The network monitoring module (NMM) is utilized by GIT framework to monitor local conditions around the sensor nodes and provide network health indicators to RM for maintaining desired reliability.

4.2.2 Framework Parameter Classification

In order to provide tunable reliability, the framework considers different parameters of interest that are used to provide reliability mechanisms. These parameters exploit temporal and spatial redundancies in the network to provide desired reliability. We identify following parameters: (a) number of sources ($\#src$), (b) number of retransmissions ($\#ret$), (c) number of paths ($\#path$), (d) number of cache points ($\#CP$), (e) information rate and (f) error codes, e.g., erasure codes. These parameters span from application to network layers and from node level to network level as shown in Figure 4.2. $\#CP$ is related to the storage of messages along the path such that in case of message loss the recovery can be initiated. It is shown that for WSN the hop-by-hop approach outperforms other approaches in terms of reliability [Wan et al., 2002]. Thus, we assume that the information is cached at

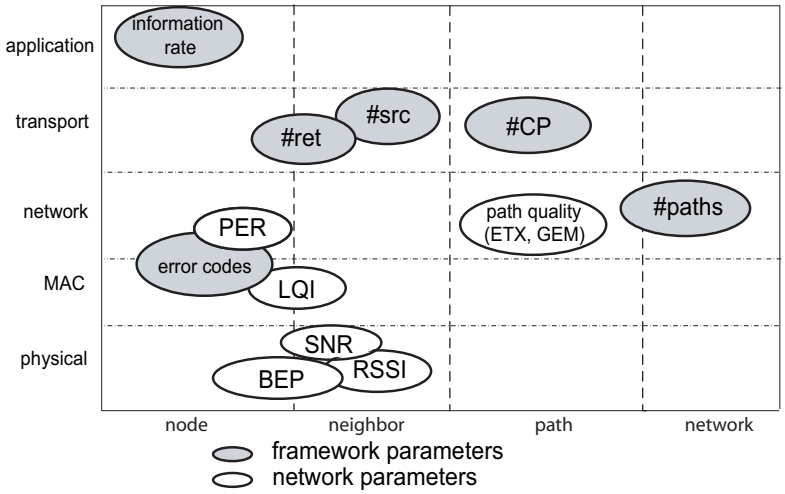


Figure 4.2: Parameter classification

each hop along the path until an ACK is received. Error codes on the other hand require very high computational power and thus are not suitable for low processing sensor nodes. In this thesis, we explore how to tune and adapt between $\#ret$, $\#path$, $\#src$ and information rate to ensure application specific tunable reliability.

Chapter 5 aims at exploring the techniques to tune $\#ret$ and $\#src$ to maintain the desired reliability requirements. Whereas, Chapter 6 utilizes $\#ret$, $\#path$ and information rate parameters to provide tunable reliability.

4.3 Information Module

IM is responsible for managing the information inside the network and accordingly selects the subset of information nodes (amongst all possible information sources) in a distributed way for further transport. IM selects information nodes based on application requirements and type of information. Sensor nodes locally identify the type of generated information based on criteria specified by the application, e.g., a clustering algorithm selects the cluster head for data collection to generate the atomic information. Such criteria specification is beyond the scope of this thesis and we assume that the type of information is specified by the application over design or deployment.

We now describe how IM selects information nodes for different types of information.

4.3.1 Node Selection for Atomic Information

If an application specifies non redundant atomic information, the sensor node becomes an information node after filtering or pre-processing of the raw data. The information entity is then handed over to RM for further processing. For non redundant atomic information the IM relies on underlying mechanisms to generate the information from the raw data and the identification of information nodes. GIT framework assumes the pre-processing steps are valid and accurate, thus the information is accurately generated.

Node Selection for Redundant Atomic Information

If the application stipulates redundant atomic information to be transported, it is not efficient to let all the sensor nodes deliver the same information. We distinguish between the redundant raw data required to generate atomic information and redundant information. For example, the event detection application may specify that redundant atomic information is generated with

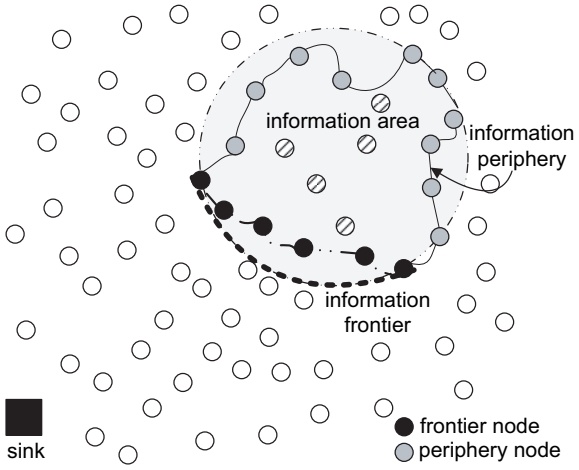


Figure 4.3: Redundant atomic information

the change in a particular attribute beyond a certain threshold. In such situations if all the sensor nodes start to send the information they will waste the inadequate resources and result in a large number of transmissions without any added benefit. In such a case a single node is sufficient to transport the redundant atomic information. Now the question is how to efficiently select a single node among several sensor nodes reporting the same information? In order to select a single information node clustering algorithms can be utilized. The major drawback of clustering is the overhead required for creating and maintaining the clusters [Abbasi and Younis, 2007], since the information generation and the corresponding information area are dynamic in nature. Furthermore, the cluster head itself may possibly be selected farthest from the sink, which requires more transmissions for information transport. We propose an efficient solution (Algorithm 1) for selecting a single sensor node to report the redundant atomic information which eliminates the redundancy with less communication steps. The main objective is to minimize the number of transmissions required to transport the information to the sink. Therefore, the basic idea is to select an information node within the information area which is closest to the sink. In order to efficiently transport the redundant atomic information, IM identifies the information periphery, i.e., the perimeter that spatially covers the information area in a distributed manner. Once the periphery is available, IM categorizes the information frontier, defined as the periphery nodes closest to the sink in terms of number of hops. Among the sensor nodes on the information frontier, an information node is selected for information transport using frontier traversal (Figure 4.3). Once the redundant atomic information

is generated at a sensor node, this node broadcasts (with some delay) the information verification message (VERIFY) to its 1-hop neighbors in order to verify the generation of information (Algorithm 1: lines 1-3). Based on neighborhood knowledge (N_u,N_d and N_e (Section 2.1)) and using approaches like Isolines [Solis and Obraczka, 2005] sensor nodes identify that whether they lay on the periphery or not. If the sensor node receives VERIFY message from all its neighbors, i.e., N_u,N_d and N_e, it belongs to the information area and concludes that it is not on information periphery. All sensor nodes enclosed in the information periphery suppress their information transport (Algorithm 1: line 4), since they are farther from the sink compared to sensor nodes on information frontier. The sensor nodes which receive VERIFY message from N_u or N_d conclude that they belong to information periphery. Additionally, the sensor nodes receiving VERIFY message from N_d lay on the information frontier. Since nodes belonging to information frontier are closest to the sink, the other periphery nodes also suppress the information transport (Algorithm 1: lines 5-9). In one message exchange inside the information area Algorithm 1 suppresses majority of sensor nodes from being selected for information transport. Next, we have to allocate a node on the information frontier that is closest to the sink for the information transport. Information frontier traversal ensures that the node which is nearest to the sink on the information frontier will be selected for information transport. To ensure that the closest node is selected, each node on the frontier sends a traversal message (SUPPRESS) along the frontier to suppress other nodes from sending redundant information. Each frontier node starts its traversal timer according to its hop distance to the sink. The shorter the distance to the sink, the earlier a frontier node starts its traversal, i.e., $t_\partial = t_o/h(X) + \mho$ where t_o is the time to send a message, $h(X)$ is the hop distance of the node to the sink, and $0 < \mho < 1$ is the random factor to avoid collisions. If a frontier Node X receives a SUPPRESS message before Node X starts its own traversal, it broadcasts the SUPPRESS message and discards its own traversal (Algorithm 1: lines 19-21). Along the frontier if the SUPPRESS message is received by a periphery node it replies the frontier node with CLEAR message. The last node on the frontier back-propagates the CLEAR message to the initiator node for information transport (Algorithm 1: lines 25-28). The initiator node starts the information transport as soon it receives the CLEAR message.

Two or more sensor nodes may start the frontier traversal if they are located at the same hop distance or due to internal clock drifts. In such a case, intermediate frontier nodes may receive more than one SUPPRESS message and decide to discard the extra SUPPRESS messages. When the initiator nodes have different hop distances, the decision of discarding a SUPPRESS

Algorithm 1: Node selection for redundant atomic information

Data: R_d, $h(X)$, $N(X)$ ←neighbors of X, $msg \leftarrow AI_r$ (redundant atomic information)

```
1  if source node and AI_r then
2  |  broadcast(verifyMsg);
3  end
4  if (X ∧ ∀ N(X) ∈ AI_r) then suppress(msg);
5  else if (X ∧ N_u ⊂ N(X) ∉ AI_r) then
6  |  suppress(msg);
7  |  peripheryNode(TRUE);
8  end
9  else if X ∧ N_e ⊂ N(X) ∉ AI_r then
10 |  suppress(msg);
11 |  peripheryNode(TRUE);
12 end
13 else if X ∧ N_d ⊂ N(X) ∉ AI_r then
14 |  frontierNode(TRUE);
15 |  frontier_traversal();
16 end
17 function frontier_traversal()
18 start traversalTimer();
19 if recieve.suppMsg and !traversalTimer() and frontierNode(TRUE)
   then
20 |  stop traversalTimer();
21 |  broadcast(suppMsg);
22 else if traversalTimer() then
23 |  broadcast(suppMsg);
24 end
25 if recieve.suppMsg and peripheryNode(TRUE) then
26 |  terminateTraversal();
27 |  forward(clearMsg);
28 end
```

message is based on the hop distance to the sink. The SUPPRESS message from the node having higher hop distance will be discarded. If both initiator nodes have a same hop distance, then the criteria for discarding is based on the number of hops traveled along the frontier, i.e., the message which traveled less hops along the frontier will be discarded by the intermediate frontier nodes. Furthermore, retransmissions are carried out in order to recover the

loss of SUPPRESS message due to collisions (Section 4.5).

Node Selection for Sparse Atomic Information

The sparse atomic information is a combination of the non redundant and redundant atomic information. For sparse atomic information, the information nodes are sparsely selected by the underlying mechanisms within the information area. For example, the clustering algorithm is used to generate non redundant atomic information by the application. In this example cluster heads are the information nodes. If the information node perceive the redundant information (application specific) during in-network pre-processing, it detects that the atomic information is sparsely generated. Upon sparse atomic information generation the information nodes (cluster heads) follow the same technique as described in Algorithm 1, where only the subset of information nodes in the information area participate to select a single information node.

4.3.2 Node Selection for Composite Information

For composite information, the main challenge is to select the information nodes according to the desired application requirements. For node selection, game based solutions [Willig and Karl, 2005] are available, but such schemes select the nodes after a certain number of iterations. These approaches cannot be utilized by GIT as the information may last for only a short time inside a WSN. Other solutions such as [Choi and Das, 2009] are very application specific. The GIT framework implements a simple heuristic (Algorithm 2) to randomly select k information nodes in order to meet the desired application reliability. The information nodes can autonomously decide whether to be selected or not according to their probability of selection, i.e., R_d (Algorithm 2: lines 1-7). The property of uniform random numbers assures that statistically $(R_d \times 100)\%$ information nodes are selected for the information transport.

Sensor nodes first identify the composite information inside the WSNs according to the application specification. Then, each node selects itself form the information area/periphery according to application requirements. For example, tracking applications may require some percentage of sensors on the periphery. Similarly, event based applications may require some nodes from the information area to report the coverage of the event [Choi and Das, 2006].

Once the sensor nodes are selected for different information types by IM for information transport, RM starts its functionality to provide desired reli-

Algorithm 2: Composite information transport

```
   Data: R_d
1  if source node and composite information then
2  |  i ← RAND[0,1]
3  |  if i >= R_d then
4  |  |  infNode();
5  |  |  transportInfo();
6  |  end
7  end
```

ability requirements. We now describe the efficient integration of our developed mechanisms (Chapter 5 and Chapter 6) such as hybrid acknowledgment, adaptive retransmissions and proactive congestion control with GIT framework. Furthermore, we present how the developed mechanisms enhance the interactions among the modules of GIT in order to ensure desired application reliability.

4.4 Reliability Module

To achieve and maintain tunable reliability, RM manages reliability allocation along the path and keeps track of information loss. If RM examines that information entity can achieve the desired reliability it passes the information to the network layer for transporting it to the next hop along the path. If the desired reliability is not attainable, RM notifies TAM for tuning and adaptation of temporal and/or spatial properties in order to maintain the desired reliability. We now discuss how the sub-modules of RM realize the task of tunable reliability.

4.4.1 Reliability Allocation Module

The multihop communication is commonly used in WSNs. Due to the nature of wireless medium and perturbations inside the network, the reliability across the hops varies. RAM is responsible for the allocation of application reliability across hops such that the information reaches the destination. For optimal allocation the information node must have a global knowledge of all intermediate hop reliabilities, which is hard to achieve in WSNs due to high communication overhead. RAM makes use of a simple heuristic to allocate the reliability across each hop along the path according to hop distance to the sink. For known R_d and number of hops from the sink, an information

node locally calculates the desired reliability requirement (R_{h_d}) at each hop as: $R_{h_d} = (R_d)^{1/h_{inf}}$ where h_{inf} represents number of hops from the information node to the sink. R_{h_d} considers a uniform reliability requirement across all hops. Each information node calculates R_{h_d} and the relay nodes along the path ensure the allocated reliability. In Chapter 5, we show other reliability allocation schemes and show that utilizing uniform reliability allocation mechanism is beneficial for achieving desired reliability.

4.4.2 Message Loss Detection Module

The main objective of MLDM is to efficiently detect the information loss due to communication perturbations. Several message loss detection techniques can be adopted to provide reliability such as ACK, NACK, IACK and timers. GIT utilizes hybrid ACK, a unique combination of IACK and explicit ACK along with probabilistic suppression of the information. When a node sends a message, it waits for an IACK to ensure the message delivery to the receiver node. After a predetermined time, if IACK is not received, the node retransmits the message. GIT also employs dynamic local retransmission timers to efficiently maximize the benefit of hybrid ACK scheme by observing the neighbor node's buffer status. As the information entity is comprised of a single message, the choice of hybrid ACK is beneficial. However, MLDM can easily integrate other strategies. For example, NACK scheme can be utilized if information consists of more than one information entity [Stann and Heidemann, 2003].

4.4.3 Congestion Control Module

Another common perturbation in WSNs is congestion due to buffer overflow, which leads to information loss. The commonly used congestion detection schemes in the WSN literature rely on monitoring (i) channel utilization, (ii) buffer utilization, and (iii) average message queuing time. These schemes are reactive in nature and lead to message loss until they stabilize. CCM comprises of a pro-active congestion detection mechanism by monitoring the information flow across each sensor node. CCM identifies three types of congestions inside WSNs, i.e., link level congestion, short lived congestion and long lived congestion. CCM triggers link level congestion avoidance using application aware scheduling of information transport. As soon as CCM detects a higher incoming information rate than the outgoing information rate, it suspects a short lived congestion. Consequently, to alleviate short lived congestion, CCM sends a request to TAM for adapting appropriate parameters. If CCM observes that the buffers of its neighbor nodes are also

full (by coordinating with NMM), it concludes that long lived congestion is prevailing and indicates TAM to adjust the information flow accordingly. Chapter 6 highlights and elaborates the functionality of CCM.

4.5 Tuning and Adaptation Module

Once the information loss is detected by RM, TAM has the responsibility to recover the desired information by tuning and adapting the reliability parameters. The reliability parameters exploit spatial and temporal properties of the network. We categorize spatial parameters as $\#src$ and $\#path$. On the other hand, temporal parameters include $\#ret$ and information rate. GIT efficiently controls the $\#src$ for atomic and composite information and avoids unnecessary transmissions using IM. When message loss is indicated by MLDM, TAM adapts $\#ret$ on-the-fly along the path if there is no congestion inside the network. When the congestion is observed by CCM, TAM adapts $\#paths$ and reduces the information rate.

Tuning Temporal Parameters

To ensure reliability across a hop (X, Y) and to tolerate perturbations more than one transmissions are required. Let $r_{(X,Y)}$ be the maximum number of transmissions required than, $r_{(X,Y)} = \frac{\log(1-R_{h_d})}{\log(1-R_{hop})}$, where R_{hop} is a hop reliability across X and Y. Each node along the path dynamically adapts r according to its local hop reliability and application requirements. If a sensor node receives an IACK it stops retransmitting.

Adapting Spatial Parameters

TAM distinguishes between short lived and long lived congestions and accordingly reacts to the situation. If CCM indicates a short lived congestion, TAM utilizes split-path and sends information to neighbor nodes. If the neighbor node is from the set N_d, it will not change the reliability allocation of RAM as the path length is not changed. If the selected neighbor is from N_u or N_e, the path length is changed and TAM indicates RAM to recalculate the reliability allocation. When CCM indicates a long lived congestion, TAM integrates multiplicative decrease policy to reduce the information rate. Once the congestion is over TAM uses additive increase policy to increase the information rate.

4.6 Network Management Module

NMM is responsible for observing the local network conditions. To monitor the network conditions the different indicators can be utilized, e.g., bit error probabilities (BEP), packet error rate (PER), signal to noise ratio (SNR), received signal strength indicator (RSSI), link quality indicator (LQI), and path estimators (ETX [Couto et al., 2005], GEM [Saukh et al., 2006]). These indicators range from locally observing link quality to network wide path qualities as shown in Figure 4.2. There is a broad research in link quality estimators [Baccour et al., 2009]. RSSI is a poor indicator of link quality [Woo et al., 2003] and LQI is specific to some radios and provide soft state of the link quality. ETX and GEM on the other hand, provide path quality which can lead to high overhead due to providing global knowledge of the route. These indicators are more suitable for static network conditions and where network connectivity is stable.

We emphasize two indicators which are readily available and provide good link estimations, i.e., link quality indicator (LQI) and bit error probabilities (BEP). LQI is on-chip indicator for link quality and is available on current mote platforms such as Micaz and TelosB. LQI is shown to be an acceptable indicator for link quality estimation [Lea et al., 2009; Polastre et al., 2005]. By contrast, BEP is available in simulation environments and also shown to be effective indicator [Dong et al., 2009]. BEP provides local conditions around the node and represents the elementary indicator for other aggregated indicators such as PER [Levis et al., 2003]. BEP reflects wide range of cases, i.e., network congestion, collisions and contention, since they tend to corrupt the message which is similar to BEP.

The modular approach of GIT allows other link quality estimators such as received signal strength indicator or expected number of transmissions to be utilized by NMM.

4.7 Chapter Summary

By introducing the generic information transport (GIT) framework this chapter established the necessary basis for GIT modules. The GIT approach provides the desired application reliability despite evolving application requirements and dynamic network conditions. GIT reduces application dependency by utilizing generic information abstraction and its ability to tune itself according to application requirements. In particular, we designed techniques to restrict redundant information as close as possible to the information area. GIT copes with a wide range of network conditions ranging from basic wire-

less links to network wide congestion by adapting between basic temporal and spatial reliability mechanisms.

Chapter 5

Exploiting Spatial Correlation for Tunable Reliability of Information Transport

The existing solutions are generally designed for specific applications and there exist only focused solutions (Chapter 3). In this chapter we provide a mechanism for the tunable reliability of information transport by exploiting inherent spatial correlation of information generated in WSN. To overcome perturbation due to dynamic network conditions and to comply with evolving application requirements an adaptive retransmission mechanism based on spatial correlation is proposed. Different heuristics are proposed to allocate the reliability across the path in order to maintain the desired reliability. Our simulation results show that the proposed solution not only provides application specific reliability, but also saves expensive retransmissions leading to energy efficient solution. This chapter provides the foundation for the reliability allocation module (Section 4.4.1), the message loss detection module (Section 4.4.2) and the tuning & adaptation module (Section 4.5) of the Generic Information Transport Framework (Chapter 4).

In particular, this chapter makes the following contributions:

- We develop an adaptable and reliable information transport approach that builds on top of RBC and ensures the tunable reliability of information transport.
- We show that the desired application requirements are maintained in the presence of perturbations by efficiently exploiting spatial correlation.
- We present and compare several reliability allocation heuristics capable

of ensuring tunable reliability along the path. We furthermore show that uniform reliability allocation has the best performance among all approaches.

The above contributions constitute one of the major contribution (**C4** - Section 1.4.2) of this thesis.

Next, we identify the lack of adaptability as main shortcoming in existing work, with particular focus on RBC. Subsequently, we propose the solution to ensure the tunable reliability of information transport by exploiting spatial correlation. Finally, the evaluation of the proposed approach is presented.

5.1 Overview

Based on the observations from comparative study in Chapter 3 we note that the existing solutions does not distinguish between different application requirements and always try to provide the high reliability. In Zhang et al. [2005] the authors provide a reliable information transport protocol termed as reliable bursty convergcast (RBC). RBC combines most of the existing reliability mechanisms by exploiting both temporal and spatial redundancies in the network. Thus, RBC results in always providing high reliability. However, RBC is not capable of adapting varying application requirements and evolving network conditions. Since RBC already implements a suite of reliability mechanisms, we aim at adapting these mechanisms to account RBC for different application requirements and dynamic network conditions.

For motivation we consider a scenario where application requires tunable reliability of information transport. In the considered case, the atomic information is generated by many sensor nodes. To this end, we consider 4 sensor nodes for sending the redundant information to the sink. We investigate the RBC's ability to adapt to dynamic network conditions and to maintain the varying desired application reliability. This is crucial for the information transport, since the network conditions may change during the lifetime of the network. We performed simulations for 25 sensor nodes with the simulation settings as described in Section 5.3. To represent different network conditions the BEP between a node and its neighbors is varied from 0 to 0.02. Figure 5.1 depicts the RBC's adaptation for different reliability requirements and evolving network conditions. For low BEP (0.0 - 0.01) RBC over performs and provides higher information transport reliability than required by

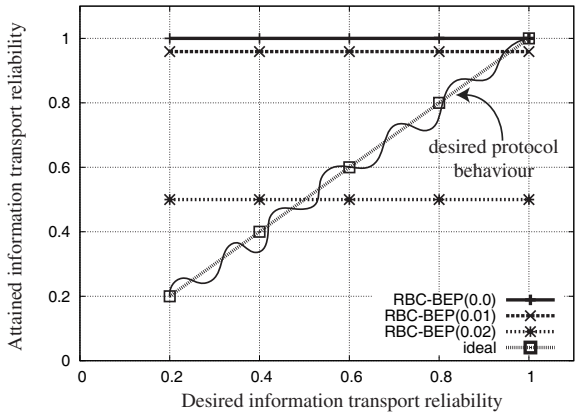


Figure 5.1: Non-adaptiveness of RBC under different network conditions

the application. This result indicates the inability of RBC to adapt to different application requirements and suggests that any information transport solution should be aware of application requirements. As BEP increases, the RBC reliability decreases, suggesting that the protocol performs poorly under erroneous network conditions and consequently does not adapt well. Although RBC by default includes a fixed number of retransmissions (commonly 2), it is not able to cope with the evolving network conditions. In general, RBC provides a constant reliability for a given network condition and thus does not adapt to varying application requirements which can be either higher or lower than the achieved reliability. This motivates for an adaptive solution which provides application specific reliability and adapts to network conditions in a way that follows the ideal case shown in Figure 5.1.

5.2 Adaptive Reliable Information Transport

In this section, first the requirements and assumptions driving our approach are described. Next, the analytical model for the information transport is developed followed by spatial adaptation for atomic information.

The proposed approach make following three assumptions about the underlying network. First, we assume that the information rate is low enough to make network congestion negligible. This is a reasonable assumption for some applications [Hartung et al., 2006; Lea et al., 2009; Werner-Allen et al., 2006]. In the next chapter we relax this assumption and develop a solution that also accounts for congestion. Our second assumption is that the snooping of messages comes at low cost in terms of energy. Therefore, a low power listening mechanism [Ye et al., 2004b] can be used resulting in low cost snooping [Woo et al., 2003]. We further assume that the contention inside the network is low. Collisions occur when two or more neighboring nodes within the interference range of each other transmit at the same time. However, for low information rates, the transmission collisions are negligible which leads to low contention. We will relax this assumption as well in the next chapter and propose an application specific contention control mechanism.

5.2.1 Analytical Model for Convergecast Reliability

In order to achieve tunable reliability of information transport, we consider two parameters, i.e., $\#src$ and $\#ret$, as introduced in Section 4.2.2. We focus on how to integrate and tune them such that the application requirements are fulfilled despite the encountered WSN node/communication level perturbations.

Let us consider a Node X sending a message corresponding to an information entity via Node Y along the path h hops away from the sink. The reliability of reaching the information from X to the sink is:

$$R_d = \prod_h R_{hop} \tag{5.1}$$

where R_{hop} is the reliability across a single hop. Since hop-by-hop reliability assurance is appropriate for WSN [Wan et al., 2002], we focus on how to enhance the information transport reliability across a hop along the path. When a message m is received at a receiver Y, the acknowledgment for m is reached back to the sender X by snooping m when it is forwarded by Y later. Accordingly, the link quality across (X,Y) will be LQ = $p_{(X,Y)}p_{(Y,X)}$, where $p_{(X,Y)}$ is the probability of sending m from to X to Y and $p_{(Y,X)}$ is the probability to snoop the acknowledgment. To ensure reliability across a hop (X, Y) and to overcome node and communication level perturbations such as message loss, more than one transmission are carried out. Let r be the number of transmissions, then the information transport reliability across a hop (X, Y) is:

$$R_{hop} = 1 - (1 - p_{(X,Y)}p_{(Y,X)})^r = 1 - (1 - LQ)^r \tag{5.2}$$

Since r is the total number of transmissions therefore $\#ret = r - 1$. For redundant atomic information many sensor nodes generate messages and send towards the sink. For redundant atomic information the source nodes typically have spatial correlation and redundant information is sent in a convergent manner to the sink. Since many sensor nodes are sending the same information to the sink, information transport reliability will not be hampered if information from some sensor nodes is lost. Accordingly, the integrated reliability across a hop will be:

$$R = 1 - (1 - R_{hop})^s \tag{5.3}$$

where $s = \#src$ transporting the information to the sink. Applying Equation (5.2) to Equation (5.3) yields

$$R = 1 - ((1 - LQ)^r)^s \tag{5.4}$$

Equation (5.4) integrates a mechanism which explicitly accounts for the spatial correlation in the form of $\#src$ and the temporal redundancy in the form of $\#ret$. It should be noted that Equation 5.4 requires that all the source nodes know $\#src$ a priori or some underlying mechanism provides $\#src$, e.g., in query based applications the query may specify the number of nodes reporting the information. For the case where $\#src$ is not known, the mechanism developed in Section 4.3 can be utilized.

5.2.2 Reliability Allocation

Usually, in WSN the information is transported over many hops from the source node to the sink. Thus, the application requirement is divided over the number of hops and is defined as follows:

Definition 5. *The hop-by-hop reliability requirement R_{h_d} ($0 < R_{h_d} < 1$) is defined by the probability of messages of Node X to be transported successfully from one hop to its next hop node along the routing path between source node and sink.*

Due to the nature of wireless medium and perturbations inside the network, the reliability across hops varies. The allocation of application reliability across hops to reach the destination is therefore necessary to achieve application specific reliability. For optimal allocation the information node must have a global knowledge of reliability across all intermediate hops. Contrary, the global knowledge is hard to achieve in WSNs due to the high communication overhead. The proposed solution makes use of a simple heuristic to allocate the reliability across each hop along the path according to hop distance to the sink. For known R_d and number of hops from the sink, an information node locally calculates the desired reliability requirement (R_{h_d}) at each hop as:

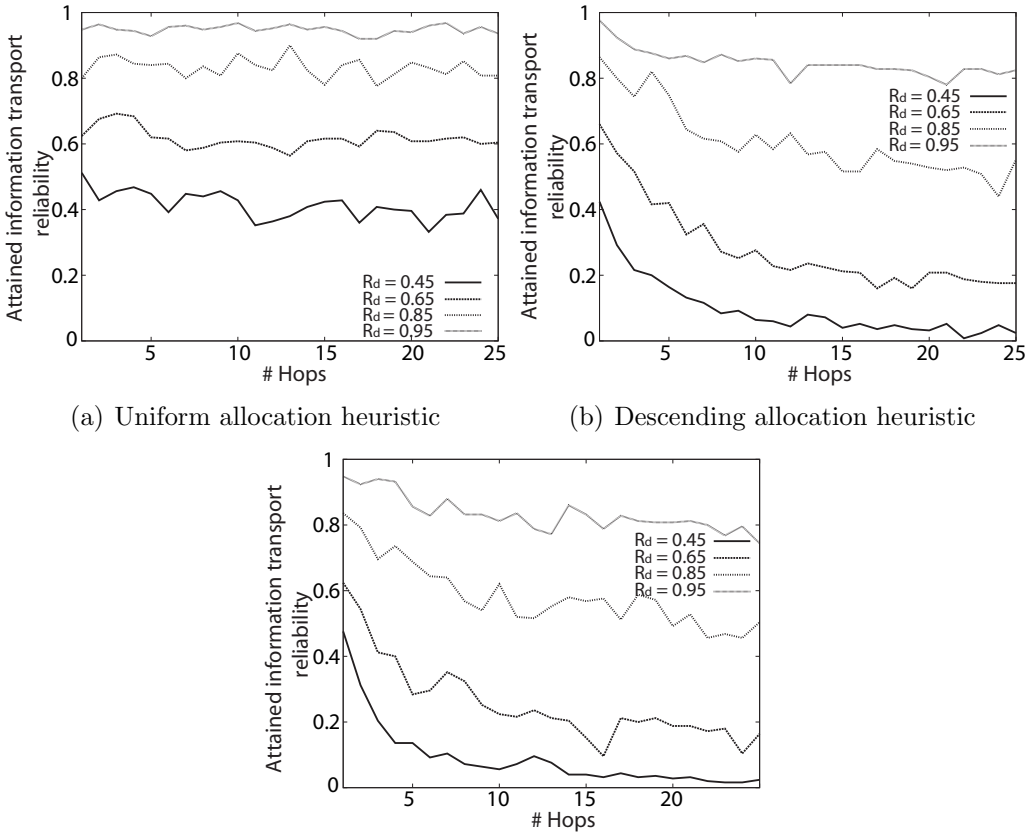
$$R_{h_d} = (R_d)^{1/h_{src}(X)} \tag{5.5}$$

where $h_{src}(X)$ represents number of hops from the source node to the sink. R_{h_d} considers a uniform reliability requirement across all hops. Each information node calculates R_{h_d} and the relay nodes along the path ensure the allocated reliability.

The second heuristic calculates R_{h_d} conditionally depending on the outcome of the previous hop. If the next hop receives the message to be sent towards the sink, it will recalculate the desired reliability for each remaining hop. This can be viewed as every node being an originator of the information. Instead of using $h_{src}(X)$, the current Node X along the path calculates R_{h_d} based on its hop distance $h(X)$ to the sink as follows

$$R_{h_d} = (R_d)^{1/h(X)} \tag{5.6}$$

In this heuristic the reliability allocation across the hops is decreasing as the information moves towards the sink. This heuristic allocates reliability in descending order as the information has traveled across the hops. Since the message has already traveled towards the sink, allocating the lower reliability to the hops near to the sink may result in information failure. This observation leads to our third heuristic where we reverse the second heuristic in



(a) Uniform allocation heuristic

(b) Descending allocation heuristic

(c) Ascending allocation heuristic

Figure 5.2: Attained reliability using different reliability allocation heuristics

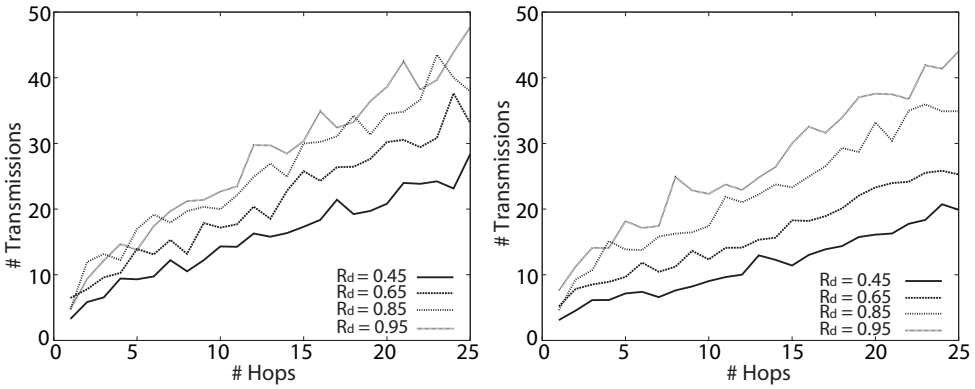
ascending order. In the third heuristic each node calculates R_{h_d} as:

$$R_{h_d} = (R_d)^{1/[h_{src}(X)-(h(X)-1)]} \tag{5.7}$$

This heuristic allocates less reliability at the start of the path towards the sink. As the message progresses towards the sink, reliability allocation is increased.

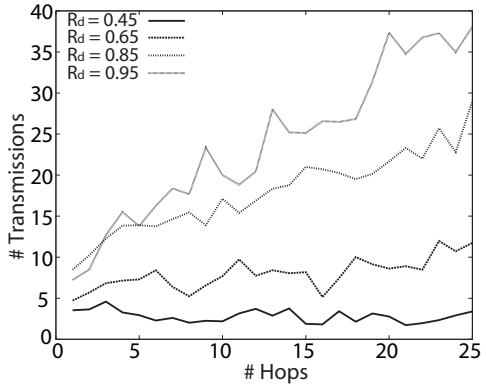
We performed high level simulations in Matlab to determine which heuristic is most appropriate for our given scenario. We utilized our retransmission strategy as described in Section 5.2.1 in simulations. For link reliability along the path we used Gaussian functions to mimics varying link reliability. Figure 5.2 depicts the impact of the path length on the overall transport reliability for the proposed heuristics. Figure 5.3 shows the number of transmissions necessary to attain the desired reliability for different heuristics. The plots clearly show that the first heuristic guarantees the required reliability independently from the source node's distance to the sink. Each

sensor node locally adjusts the number of required retransmissions to meet R_{h_d}. For the second heuristic, the overall attained reliability degrades at each step as R_{h_d} degrades. Longer paths result in a greater accumulation of R_{h_d} degradation. Since the third heuristic is a reverse case of second heuristic, we observe similar results. Generally, for the first heuristic the number of transmissions is slightly higher resulting from the tradeoff made to attain the desired application reliability.



(a) Uniform allocation heuristic

(b) Descending allocation heuristic



(c) Ascending allocation heuristic

Figure 5.3: Number of transmissions using different reliability allocation heuristics

5.2.3 Adaptation for Redundant Atomic Information

Our solution adapts temporal redundancy corresponding to the evolving application requirements and dynamic network conditions to overcome the perturbations. Algorithm 3 depicts the adaptation for redundant atomic information. The source node calculates and includes R_{h_d} in a message using

uniform reliability allocation heuristic. Next, the source node forwards the message to the next hop along the path (Algorithm 3: lines 2-4). When the node forwards a message it first decides with probability p_s whether to send the message or not (Algorithm 3: line 14). The decision is based on the source node's local network condition, i.e., link reliability (R_L) and R_{h_d}, as follows:

$$p_s = \begin{cases} R_{h_d}/R_L & \text{if } R_L > R_{h_d} \\ 1 & \text{if } R_L \leqq R_{h_d} \end{cases} \tag{5.8}$$

Algorithm 3: Adaptation for redundant atomic information

```
   Data: R_d, R_L, h, msg, Y_i←next hop along the path
 1 if source node and redundant atomic information then
 2 |  calculate R_{h_d} using Equation (5.5);
 3 |  msg.R_{h_d} ←R_{h_d};
 4 |  transport(msg, Y_i);
 5 end
 6 if forwarding node then
 7 |  if msg already in buffer then
 8 |  |  purge received msg;
 9 |  end
10 |  R_{h_d} ← msg.R_{h_d};
11 |  transport(msg, Y_i);
12 end
13 function transport(msg, Y_i):
14 check whether to send or suppress using Equation (5.8);
15 if send then
16 |  calculate r using Equation (5.9);
17 |  send msg to Y_i; if snoop IACK then
18 |  |  purge msg from buffer;
19 |  |  exit();
20 |  end
21 end
22 if suppress then
23 |  purge msg from buffer;
24 end
25 end function
```

If $R_L > R_{h_d}$ the source node sends the message with probability $p_s = R_{h_d}/R_L$ in order to maintain the required application reliability. For the case $R_L \leqq R_{h_d}$ the source node always sends the message. This step ensures that the proposed solution always maintains the specified information transport reliability thus adapting to application requirements.

Once the node decides to send the message, it will calculate how many transmissions are required to fulfill the application requirements. The node checks whether $R_{int} \geqq R_{h_d}$, when true it will transmit the message once to its parent node else the node will calculate the number of transmissions required to attain R_{h_d} (Algorithm 3:lines 15-21), using Equation (5.4).

$$r = \begin{cases} \frac{log(1-R_{h_d})}{s \cdot log(1-LQ)} & \text{if } R_{int} < R_{h_d} \\ 1 & \text{if } R_{int} \geqq R_{h_d} \end{cases} \tag{5.9}$$

For r we have chosen probabilistic transmissions [Deb et al., 2003a], i.e., if $r = 1.34$ than the node will do one transmission and then another retransmission with a probability of 0.34. This minimum upper bound is important for the less number of transmissions. Using Equation (5.9) the approach ensures the desired reliability of information transport across a hop by exploiting spatial correlation. To avoid infinite transmissions applications can specify the maximum threshold r_{th} after which the sensor node will discard the message.

Proposition 5.2.1. *The minimum number of transmissions for a redundant atomic information (T^{min}_{RAI}) consisting of s sources to be delivered with application reliability R_d from Node X having message delivery probability $p(X, X+1)$ across its neighbor Node X+1 towards the sink along the path having h hops is*

$$T^{min}_{RAI} = \sum_{X=0}^{h} \frac{log(1-(R_d)^{1/h_{src}(X)})}{s * log(1-p_{(X,X+1)})}$$

Proof. An information entity generated at Node X is forwarded to the next hop Node $X+1$ if it has been successfully received regardless of the IACK outcome. Therefore, the information transport only relies on the forwarding probability $p_{(X,X+1)}$, yielding Proposition 5.2.1 as a sum over h hops similar to the derivation of Equation 5.9.

□

Proposition 5.2.2. *The total number of transmissions for a redundant atomic information entity T_{RAI} to be delivered with application reliability*

R_d from Node X to a sink along the path having h hops is

$$T_{RAI} = \frac{log(1-(R_d)^{1/h_{src}(X)})}{s * log(1-p_{(X,X+1)}p_{(X+1,X)})} + \sum_{i=1}^{h-2} \frac{log(1-(R_d)^{1/h_{src}(X)})}{s * log(1-p_{(i,i+1)}p_{(i+1,i)}p_f)} + \frac{log(1-(R_d)^{1/h_{src}(X)})}{s * log(1-p_{(h-1,0)}p_{(0,h-1)})}$$

Proof. The source node transmits until the information entity and its forwarding transmission are both received at node X and $X+1$ respectively. Following Equation 5.9, the number of transmissions required at source node is given by:

$$\frac{log(1-(R_d)^{1/h})}{s * log(1-p_{(X,X+1)}p_{(X+1,X)})} \tag{5.10}$$

The forwarded message from Node X successfully received by the next hop Node $X+1$, may not be overheard by Node X triggering a retransmission. This is accounted for the spatial dependency with conditional probability p_f = Pr[success at $X-1$ | success at $X+1$] = Pr[success at $X+1$ | success at $X-1$]. For $h-1 < X < 1$, assuming proper setting of the retransmission timeouts, the forwarding Node X, transmits until the information entity is successfully received by both, Node $X-1$ and Node $X+1$, as well as the forwarding by Node $X+1$ is snooped by Node X. Thus, the number of transmissions is given by:

$$\sum_{i=1}^{h-1} \frac{log(1-(R_d)^{1/h})}{s * log(1-p_{(i,i+1)}p_{(i+1,i)}p_f)} \tag{5.11}$$

The sink node, $X = 0$, needs to transmit an EACK. Thus the number of transmissions for the last hop will be:

$$\frac{log(1-(R_d)^{1/h})}{s * log(1-p_{(h-1,0)}p_{(0,h-1)})} \tag{5.12}$$

Combining Equation (5.10) - (5.12) yields Proposition 5.2.2. □

5.2.4 Parameter Acquisition

In order to acquire hop count h and specified desired reliability R_d, the underlying routing protocol can be utilized. The sink periodically sends beacon messages to all nodes such that a routing tree rooted at the sink is maintained. The sink includes a hop counter to beacon messages, which

allows nodes to update their hop count to the sink. In this way all nodes inside a network know how far they are from the sink (in terms of number of hops). Furthermore, a change request for the application requirement on R_d can be disseminated to the sensor nodes, e.g., through piggy backing to beacon messages. This can be further optimized by sending R_d to only a subset of nodes inside the network. It should be noted that we emphasize on information transport from sensor nodes to the sink and not on dissemination of application requirements to sensor nodes. To this end the sink can use existing reliable downstream dissemination strategies, e.g., [Park et al., 2004; Tezcan and Wang, 2007; Wan et al., 2002] to distribute the R_d.

Node X keeps track of the link quality between its parent Node Y towards the sink using Exponentially Weighted Moving Average (EWMA) [Woo et al., 2003] as follows:

$$LQ^t = (1 - \alpha) * LQ^t + \alpha * LQ^{t-1} \tag{5.13}$$

where α is a weight-factor ranging between $0 < \alpha < 1$ and LQ^t is the latest observation of the link quality in terms of BEP. The EWMA approach avoids the wrong node decisions due to sudden or abrupt changes in the network environment. In this work, a node keeps track of BEP between itself and its parent upon reception of a message or when it snoops the channel for acknowledgement.

5.3 Performance Evaluation

In order to evaluate our proposed approach, we first describe the methodology and simulation settings. Next, the simulation results are discussed for a wide representative range of operational network conditions and parameters.

5.3.1 Methodology and Simulation Settings

We define our approach as Adaptive Reliable Information Transport (AReIT). As RBC uses by default the Logical Grid Routing (LGR) [Choi et al., 2006] protocol, we continue using LGR with the default settings as described in [Choi et al., 2006]. LGR is a proactive protocol which finds the path in advance for all source and destination pairs and periodically exchanges topology information to maintain them. The source code of RBC is available for the mica2 mote platform, consequently we ported it to run under the TOSSIM environment.

The topology used in the simulations consists of a n x n grid topology. The distance between two nodes is 10 units. The sink is located at one cor-

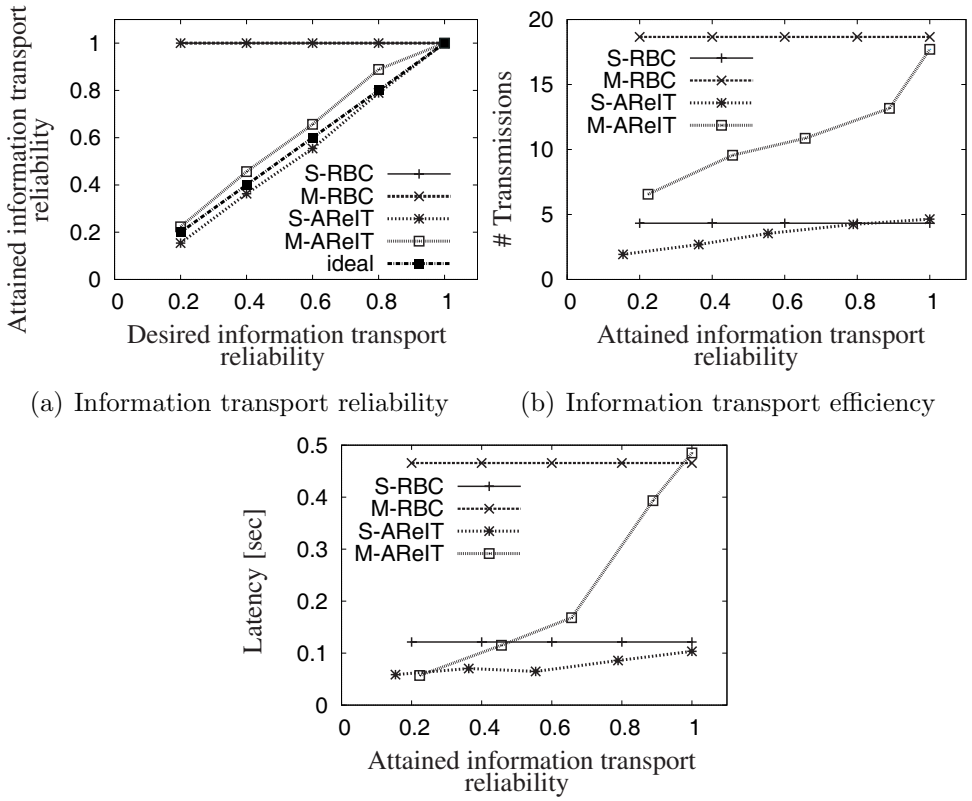
ner. The redundant atomic information is generated from another corner and transported towards the sink. Two cases are chosen: One where atomic information is generated by a single source and another where the non redundant atomic information is generated by s sources that are geographically close to each other. We termed S-RBC and S-AReIT, when the single information node sends non redundant atomic information. Similarly, we term M-RBC and M-AReIT when multiple nodes send redundant atomic information to the sink. For the experiments, 100 atomic information entities are generated with the gap of 3 sec, to be transported towards the sink. Information is generated after 10 sec from the start of the simulation to give the network sufficient time to stabilize before information is generated. For α a typical value of 0.1 as suggested in [Ee and Bajcsy, 2004] is used.

5.3.2 Simulation Results

We present our simulation results for different studies that we conducted regarding the impact of tunable reliability, network conditions, number of nodes and number of information nodes.

Tunable Reliability of Information Transport

Figure 5.4 shows the adaptation of our approach to variable application requirements on information transport. Figure 5.4 (a) depicts the reliability attained by RBC and AReIT. We observe that S-AReIT and M-AReIT attain desired reliability with a slight difference. The reliabilities attained by S-RBC and M-RBC are independent of the desired reliability and are constant. Figure 5.4 (b) shows the total number of transmissions required to attain the information transport reliability. The number of transmissions for S-RBC and M-RBC do not change. The number of transmissions varies for S-AReIT and M-AReIT in proportion to the attained level of reliability. We observe that M-AReIT corresponding to M-RBC, has relatively less transmissions due to explicitly integrating the spatial redundancy. Generally, AReIT adapts to the desired application requirements with fewer number of transmissions than RBC. Figure 5.4 (c) shows the timeliness of RBC and AReIT. The latency of AReIT is well below that of RBC for providing attained application reliability. For higher application reliability requirement (100%), AReIT behaves similar to RBC in terms of efficiency and timeliness. On the other hand, for all other cases AReIT outperforms RBC with respect to responsiveness and efficiency.



(a) Information transport reliability

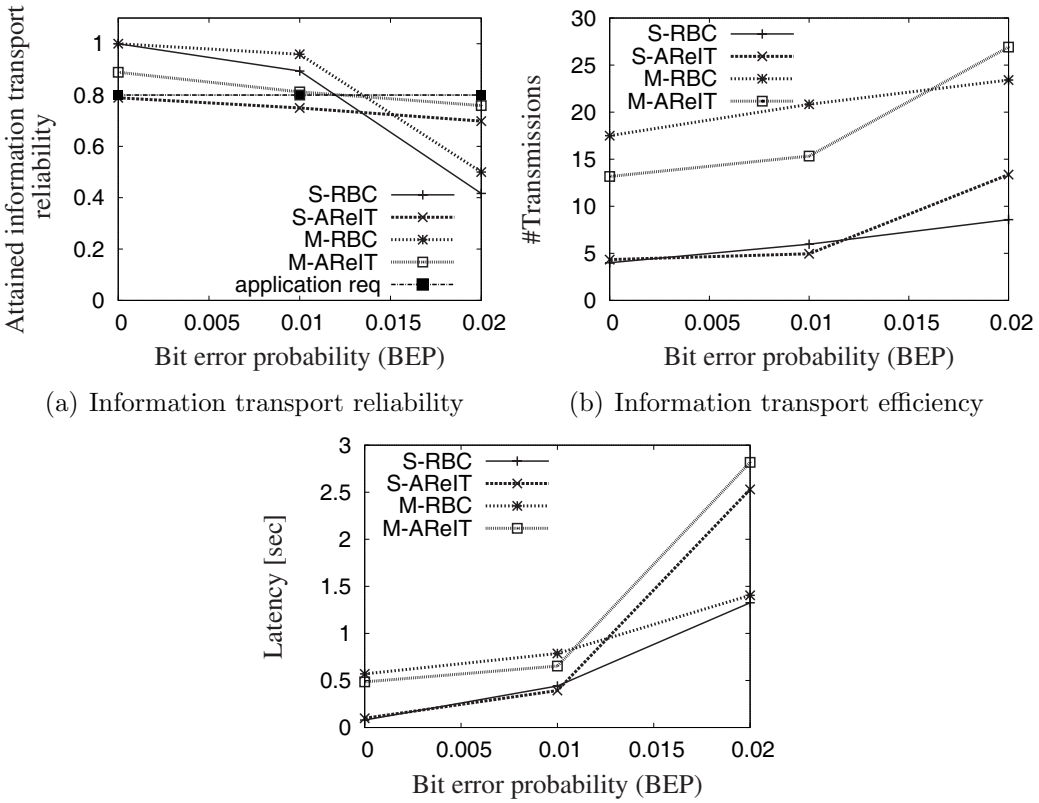
(b) Information transport efficiency

(c) Information transport timeliness

Figure 5.4: Adaptation to application requirements

Adaptation to Network Conditions

Figure 5.5 compares the robustness of RBC and AReIT under evolving network conditions. In this scenario we assume that the application requirement for the reliability of information transport is 80%. Figure 5.5 (a) shows the information transport reliability for varying BEP. S-AReIT and M-AReIT cope with the evolving network conditions and provide desired application requirement with slight difference of (+/-) 2% whereas S-RBC and M-RBC are not able to cope with evolving network conditions and provide high reliability for good network conditions (BEP 0.0 - BEP 0.01) and less reliability for worse network conditions (BEP 0.02). For BEP 0.02, M-AReIT and S-AReIT utilize more transmissions owing to the adaptation to bad network conditions by increasing the number of retransmissions (Figure 5.5 (b)). On the other hand, S-RBC and M-RBC after a fixed number of retransmissions failed to transport the information, resulting in fewer number of transmissions and achieving less than the desired reliability. This also impacts the



(a) Information transport reliability

(b) Information transport efficiency

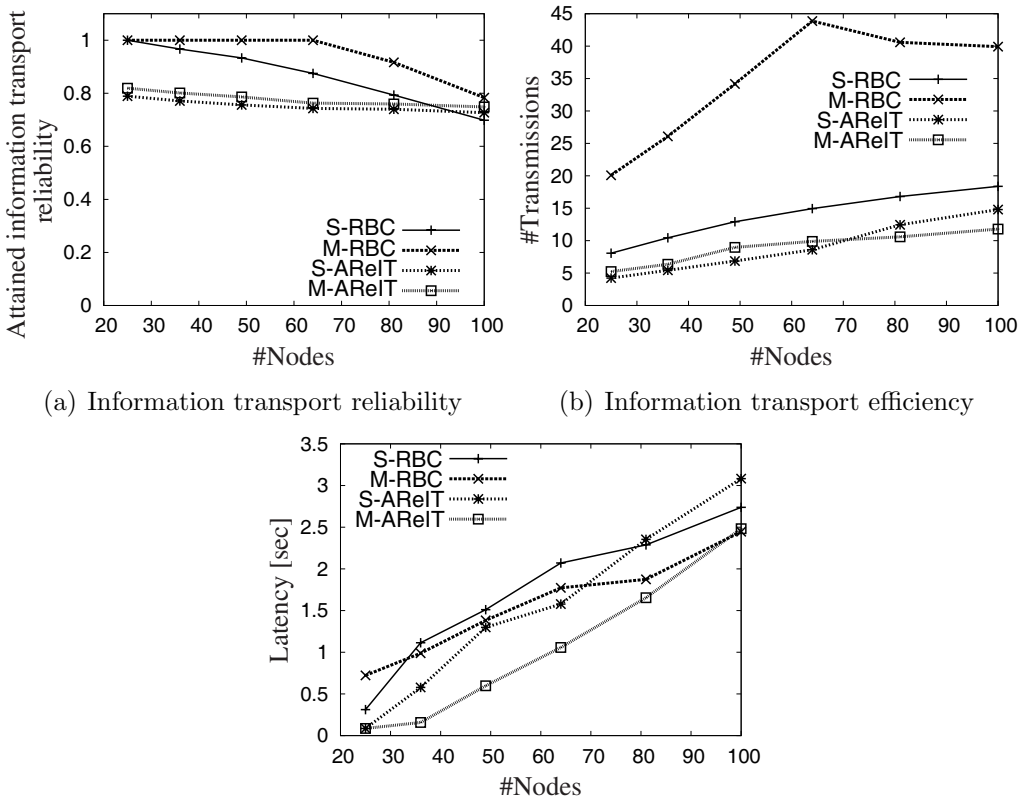
(c) Information transport timeliness

Figure 5.5: Adaptation to network conditions

timeliness of AReIT as shown in Figure 5.5 (c). At BEP 0.02 the latency of S-AReIT and M-AReIT is higher than S-RBC and M-RBC, but it is directly related to the number of transmissions and attained reliability. In general, AReIT always maintains the desired application reliability.

Adaptation to Network Size

Figure 5.6 depicts the impact of the number of sensor nodes on AReIT and RBC. This study helps in understanding how efficiently AReIT scales corresponding to the number of sensor nodes. In this scenario we assume that the application requirement for information transport is 80%. Figure 5.6 (a) shows the reliability achieved by RBC and AReIT for both redundant and non redundant atomic information. It should be noted that with increasing number of nodes the number of hops also increases. The reliability of M-RBC gradually decreases as the number of sensor nodes is increased. For S-RBC we observe a similar trend. The longer routes hinder the reliability



(a) Information transport reliability

(b) Information transport efficiency

(c) Information transport timeliness

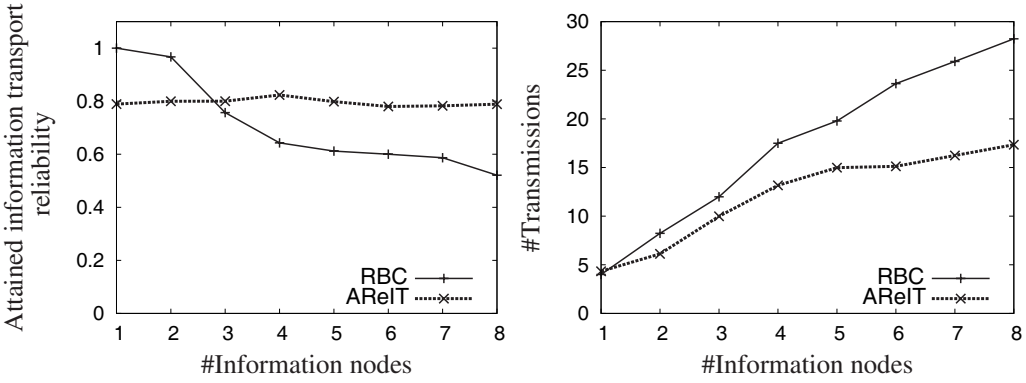
Figure 5.6: Adaptation to network size ($R_d = 0.8$)

of RBC due to its fixed number of retransmissions. As the number of hops increases the probability of information loss also increases. Therefore, the fixed number of retransmissions does not help much in maintaining the reliability for RBC resulting in a gradual decrease of reliability. For S-AReIT and M-AReIT, the reliability is always close to the desired application reliability due to a localized adaptive retransmission strategy and the opportunistic suppression of information. From Figure 5.6 (b) it is evident that M-AReIT is more efficient than all other approaches since it exploits the spatial correlation along with adaptive retransmissions. It is noteworthy that as the number of hops increases, the number of transmissions for S-AReIT increases compared to M-AReIT, since only a single information node is sending the information (no spatial correlation is exploited). Figure 5.6 (c) depicts the direct impact of the number of transmissions on the latency, i.e., more transmissions entail a higher latency. Generally, we observe that as the number of hops increases the latency also increases. Also, the latency of non redundant

atomic information is higher than the redundant atomic information because the information may reach from any of the sensor nodes in case of redundant atomic information.

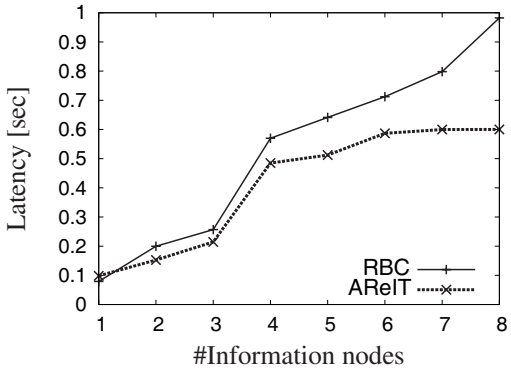
Adaptation to Number of Information Nodes

Figure 5.7 depicts the impact of number of information nodes for redundant atomic information. In this scenario, we assume that the application requirement for information transport is 80%. Figure 5.7 (a) shows the information transport reliability for a varying number of information nodes. As the number of information nodes increases, the reliability of RBC decreases. This is because RBC does not exploit the spatial redundancy of the information resulting in collisions. In contrast, AReIT adapts according to the number of source nodes resulting in less collisions and maintaining the desired reliability. The collisions for RBC trigger the retransmissions resulting in higher



(a) Information transport reliability

(b) Information transport efficiency



(c) Information transport timeliness

Figure 5.7: Impact of number of sources on redundant atomic information ($R_d = 0.8$)

number of overall transmissions compared to the AReIT as shown in Figure 5.7 (b). It is observed that the number of transmissions for AReIT is always less than RBC and with the increasing number of information nodes it is more evident that AReIT efficiently achieves the desired application requirements and exploits spatial correlation. Figure 5.7 (c) shows the impact of more transmissions with high latency of RBC compared to AReIT. AReIT does not use inherent timeliness mechanisms but its lower latency shows the impact of appropriately using the spatial correlation.

Discussions

The different simulations have quantified the viability of AReIT. In the light of the experimental analysis we make the following observations:

- Different application classes impose different reliability requirements for information transport. Thus, the approach should adapt accordingly. AReIT shows its capability of providing application specific reliability (Figure 5.4 (a)) and outperforms the RBC protocol.
- In WSN perturbations are the norm rather than the exception and providing reliable information delivery is difficult. We observed AReIT's capability to cope with harsh environments where network connectivity is fluctuating (Figure 5.5 (a)).
- The availability of information at the sink is important for reliable information transport. AReIT manages information availability by efficiently tuning the number of retransmissions and adapting to the number of information nodes.
- For the reliable information transport, timeliness plays an important role. Information not reaching to the sink in timely fashion is useless for an application, thus hindering the information transport. Figure 5.4 (c) - 5.5 (c) show that AReIT provides the required information transport reliability with low latency.
- Generally, we observe that there is a tradeoff between efficiency and timeliness to provide reliable information transport. For example, at BEP 0.0 less transmissions are carried out with low latency. On the other hand at BEP 0.02 more transmissions are required leading to a higher latency.
- The localized mechanisms utilized by AReIT ensures the scalability of the proposed solution (Figure 5.6).

- Also, AReIT adapts efficiently with the increasing number of source nodes for redundant atomic information.
- Overall, AReIT saves valuable retransmissions by maintaining the desired reliability and keeping the latency low.

5.4 Chapter Summary

In this chapter, we presented an Adaptable Reliable Information Transport (AReIT) approach for redundant atomic information. AReIT provided dynamic adaptive retransmissions corresponding to spatial correlation to overcome perturbations. We showed that AReIT is capable of adapting to different application requirements by exploiting temporal and spatial redundancies in the network. To ensure tunable reliability we argued for the reliability allocation along the path and presented various heuristics. The uniform reliability allocation performed well compared to other reliability allocation mechanisms. Finally, this chapter experimentally validated AReIT by showing promising results for evolvable application requirements and dynamic network conditions.

Chapter 6

Congestion Aware Tunable Reliability of Information Transport

In this chapter, we present a new approach called as Reliable Congestion Aware Information Transport (ReCAIT) that targets tunable reliability with congestion control for information transport in WSNs. To provide application-specific tunable reliability, ReCAIT efficiently integrates probabilistic adaptive retransmissions, hybrid acknowledgment and dynamic retransmission timer management. ReCAIT pro-actively alleviates the network congestion by opportunistically transporting information on multiple paths. If congestion persists, then ReCAIT utilizes back-pressure mechanism triggers the information rate control. ReCAIT fulfills application reliability requirements locally, which is desirable for scalability and adaptability to large scale WSNs. Our simulation results show that ReCAIT provides tunable reliability, which maximizes the efficiency of information transport in terms of energy and bandwidth.

To the best of our knowledge we are the first to target *tunable* information transport reliability with congestion awareness in face of varied application requirements and evolving network conditions. Specifically, we enhance our approach Adaptive Reliable Information Transport (AReIT) in Chapter 5 by including Hybrid ACK (HACK) mechanism and local timer management to ensure tunable reliability and provide a comprehensive congestion control mechanism. The new aspects of ReCAIT are four folds. First, we identified the problem of IACK loss in AReIT which resulted in HACK for ReCAIT. Second, for AReIT retransmission timers are managed at the source node by observing the buffer status of the receiver node only. In contrast, ReCAIT observes the buffer status of all its neighbors in order to efficiently and

pro-actively adjust the retransmission timer and to alleviate the congestion. Third, ReCAIT provides statistical bounds for reliable information transport and through simulations we showed that the information transport is always statistically bounded. Finally, ReCAIT provides congestion control on the fly by adapting pro-actively between single and multiple paths. This chapter provide message loss detection module (Section 4.4.2), tuning & adaptation module (Section 4.5) and congestion control module (Section 4.4.3) of the Generic Information Transport Framework (Chapter 4).

On the above background this chapter makes the following specific contributions.

- We develop a Reliable Congestion Aware Information Transport (ReCAIT) approach to ensure the desired reliability despite evolving application requirements and network conditions.
- We develop localized mechanisms, such as hybrid acknowledgment and retransmission timers, to achieve tunable reliability of information transport.
- We develop an efficient mechanism for mitigating wireless link congestion.
- We develop a simple yet generic mechanism, which pro-actively detects and mitigates short lived congestion in order to maintain the desired reliability requirements.
- We develop a mechanism to locally detect long lived congestion and inherently provide a back-pressure scheme to reduce information rate.

The above contributions constitute one of the major contribution (**C5** - Section 1.4.2) of this thesis. Next, the overall ReCAIT approach is presented. Subsequently, we show how to achieve the tunable reliability in non congested scenario. Consequently, for congested scenario the approach is extended followed by the detailed evaluation of ReCAIT approach. Finally, the summary of the chapter contributions appear.

6.1 Overview

The primary motivation behind ReCAIT is to provide the desired reliability of information transport despite evolving application requirements and network conditions. ReCAIT tunes the temporal parameter, i.e., number of retransmissions, and adapts the spatial parameter, i.e., number of paths, to provide congestion aware tunable reliability of information transport. The basic idea of ReCAIT approach is very simple. When there is no congestion inside the network ReCAIT tolerates the message loss by adapting the number of retransmissions and provides tunable reliability. To ensure desired application reliability, ReCAIT utilizes a Hybrid ACK scheme and retransmission timer management. Nodes proactively monitor the information flow across themselves and detect congestion by observing high information rate (an indication for short lived congestion). Due to high information rate wireless link congestion (i.e., contention) builds up. To overcome contention ReCAIT provides application-aware reliability based scheduling. When a node detects short lived congestion, it splits the information across its neighbors (potentially creating multiple paths) in order to tolerate message loss. If the congestion still persists, ReCAIT detects long lived congestion by observing the buffer status of neighboring sensor nodes. To mitigate long lived congestion ReCAIT utilizes the a back-pressure mechanism (without any extra overhead) to inform the source nodes to adjust their information rate.

Next we detail the ReCAIT mechanisms by progressively defining the elements of (a) tunable reliability (Section 6.2) and (b) congestion awareness (Section 6.3).

6.2 Tunable Reliability in Non-congested Scenario

In order to achieve the tunable reliability of information transport we propose a simple solution (Algorithm 4). If a sensor node has information to send, it first checks if the attained reliability is in accordance with the desired application reliability. If yes then to maintain the desired reliability the information us sent with a given probability. If no, then compute the number of transmissions required to attain the desired reliability for sending the information. ReCAIT utilizes the default single path (SP) for transporting the information when there is no congestion inside the network. Despite the absence of congestion, collisions are the norm in WSNs due to the commonly used CSMA-based access to the wireless medium. In order to provide tunable reliability and to tolerate message loss due to collisions along SP, ReCAIT

exploits temporal redundancy and adapts the number of retransmissions according to R_d and network conditions. For the known R_d and number of hops from the sink, a sensor node can calculate the desired reliability requirement across a hop as described in Section 5.2.2.

$$R_{h_d} = (R_d)^{1/h_{src}(X)} \tag{6.1}$$

Equation (6.1) considers a uniform reliability requirement across the hops along the path. R_{h_d} is the reliability requirement assigned to the hops by the source node along the path. The source node includes R_{h_d} inside the message when it is transported to the next hop.

Now let us consider Node X transporting information via Node Y along a SP, h hops away from the sink. To ensure reliability across the hop (X, Y) and to tolerate node and communication level perturbations, i.e., message loss, more than one transmissions are required. Let r be the number of transmissions required then the attained information transport reliability $R^A_{h_d}$ across a hop will be:

$$R^A_{h_d} = 1 - (1 - R_{hop})^r \tag{6.2}$$

where R_{hop} is the reliability across a hop along the path. Since r is the total number of transmissions, the number of retransmissions is $\#ret = r - 1$.

When a sensor node has information to transport, it first decides with probability p_s whether to send the information to the next hop or suppress it in order to maintain R_d. The decision is based on node's local network conditions and application requirements, i.e., R_{hop} and R_{h_d} as follows:

$$p_s = \begin{cases} R_{h_d}/R_{hop} + \Delta_{th} & \text{if } R_{hop} > R_{h_d} \\ 1 & \text{if } R_{hop} \leqq R_{h_d} \end{cases} \tag{6.3}$$

where $0 < \Delta_{th} \ll 1$ and is specified by the application to ensure that the attained information transport reliability is always statistically bounded between R_d and $R_d + \Delta_{th}$. When $R_{hop} > R_{h_d}$ the sensor node sends the information with probability $p_s = R_{h_d}/R_{hop} + \Delta_{th}$ in order to maintain the required information transport reliability. For $p_s = 1$ the source node always sends the message to its next hop along the path. Once the decision of sending the information is taken by the sensor node it calculates the maximum number of transmissions required to maintain the R_{h_d}. Since we require $R^A_{h_d}$ to be equal to R_{h_d}, we equate Equation (6.1) and Equation (6.2) to calculate r as follows:

$$r = \lceil \frac{\log(1 - (R_{h_d}))}{\log(1 - R_{hop})} \rceil \tag{6.4}$$

Note that at each hop along the SP, the nodes dynamically adapt r to compensate for the decisions made at the previous hop to ensure R_d.

As a simple overview, Algorithm 4 proceeds with local calculation of R_{h_d} for source node or forwarding node (Algorithm 4: lines 1-6) and determines whether to forward the information or suppress it (Algorithm 4: line 16). Once the node decided to send the information, it is wasteful to send r transmissions if the next hop node has already received the information. To mitigate this ReCAIT proposes a hybrid acknowledgment scheme and local timer management to ensure R_d across the entire path. Further operations of Algorithm 4 are detailed in the subsequent sections.

6.2.1 Hybrid Acknowledgment Scheme

In order to achieve reliability ReCAIT proposes hybrid ACK mechanism. When a node sends a message, it waits for an ACK to ensure the reception of message by receiver node. After a predetermined time if ACK is not received, the node retransmits the message. ACK requires an extra transmission in order to ensure reliability and may lead to an ACK explosion problem. In order to increase efficiency, ReCAIT takes advantage of the broadcast nature of the WSN to snoop IACK. A sender Node X starts a retransmission timer after sending information to the next hop Node Y (Algorithm 4: lines 21-22). If Node X snoops the IACK it discards the retransmission timer and purges the information from the buffer. If Node X does not snoop the information before the timer expires, it retransmits the information to Node Y (Algorithm 4: lines 24-28). If Node Y decides to suppress the message to maintain the R_{h_d} as discussed earlier (Equation (6.3)), it sends EACK back to Node X (Algorithm 4: lines 31-35). Since Node Y decides to suppress the message and Node X is unaware of it, Node X retransmits the information after the predetermined retransmission timer as it did not receive any IACK. Using this hybrid scheme (combination of IACK and EACK), ReCAIT saves the extra retransmissions carried out by Node X since it did not hear the IACK due to suppression at Node Y. Furthermore, in order to avoid IACK loss, i.e., if the information is forwarded by Node Y and Node X was not able to receive it, Node Y keeps the message for random time greater than or equal to retransmit timer (as discussed in 6.2.2) before purging it (Algorithm 4: lines 7-11). If during this time Node Y receives the message from Node X it replies with an EACK to Node X.

Next we present how to calculate retransmission timer for the affective utilization of hybrid ACK mechanism.

Algorithm 4: Tunable Reliability by ReCAIT

Data: R_{h_d}, $h(X)$, t_{ret}, msg, Y_i←next hop along the path
if *(source node)* **then**
  calculate R_{h_d} using Equation (6.1);
  $msg.R_{h_d} \leftarrow R_{h_d}$;
  transport(msg, Y_i, FALSE);
end
if *(forwarding node)* **then**
  if *(msg in buffer)* **then**
    send EACK;
    wait random time $\geq t_{ret}$;
    purge msg;
  end
  $R_{h_d} \leftarrow msg.R_{h_d}$;
  transport(msg,Y_i,FALSE);
end
function transport(msg, Y_i, *congestion*):
\\ check - send or suppress using Equation (6.3);
if *send* **then**
  calculate r using Equation (6.4);
  for *each* t_{ret} *fired* **do**
    send msg to Y_i;
    if *(congestion)* **then** start t_{ret} using Equation (6.5); **else**
      start t_{ret} using Equation (6.6);
    end
    if *(snoop IACK)* **then**
      stop t_{ret};
      purge msg from buffer;
      exit();
    end
  end
end
if *(suppress)* **then**
  send EACK;
  wait random time $\geq t_{ret}$;
  purge msg from buffer;
end
end function

6.2.2 Local Timer Management

Retransmission timers directly impact the number of transmissions. Large timeout values of timers tend to increase information transport delay, whereas small timeout values tend to cause unnecessary retransmissions. To provide reliable information transport, we design a simple and localized mechanism to manage the retransmission timers. Ideally, Node X should adapt the retransmission timer according to the buffer status of next hop node. Since the number of messages in the next hop node keep changing, the delay in forwarding a received message by Node Y also keeps changing, which leads to varying delay in IACK. In order to accurately estimate the retransmission timer, sensor nodes piggyback their buffer occupancy (q_o) while transporting the information. Node X keeps track of q_o by snooping. After sending information to Node Y (Algorithm (4): line 15), Node X calculates the retransmission timer (t_{ret}) based on the buffer occupancy of Node Y (q_{o_Y}) as follows

$$t_{ret} = q_{o_Y} \cdot t_o \tag{6.5}$$

where t_o is the time to send a message by Node X. Once a node detects congestion due to high information rate as discussed in Section 6.3.1, it will calculate the retransmission timer as follows:

$$t_{ret} = q_{o_Y} \cdot (t_o + 4t'_o) \tag{6.6}$$

where the deviation $4t'_o$ is utilized to alleviate and improve the variation of t_o when information rate is high [Jacobson, 1988; Zhang et al., 2005]. t_o and t'_o are calculated using EWMA approach as follows:

$$t_o = t_o(1 - \alpha) + \alpha t_{latest}$$

$$t'_o = t'_o(1 - \alpha) + \alpha(t_{latest} - t_o)$$

where t_{latest} is the latest observation of t_o. Algorithm 4 efficiently tolerates the information loss due to collisions by using hybrid ACK and retransmission timers with appropriate timeout values. Algorithm 4 also ensures desired tunable reliability by suppressing the information transport and adapting the number of retransmissions.

Now we elaborate ReCAIT congestion awareness approach and present algorithms for short (Algorithm 5) and long lived congestion (Algorithm 6) inside the network. We also show how ReCAIT provides reliability and application-aware contention resolution in order to avoid information loss.

6.3 Congestion Control

ReCAIT utilizes proactive congestion detection in order to tolerate the information loss. Once the congestion is detected ReCAIT provides mechanisms to mitigate the congestion in efficient manner by dispersing the information to the neighbor nodes. ReCAIT continuously monitors the network condition and provides information rate adaptation for source nodes without explicit notification. Sudden burst of information leads to high information rate, which consequently causes the congestion inside the WSN [Jaewon et al., 2007]. In such situation, the incoming information rate (ξ_i) across a node is high compared to the outgoing information rate (ξ_o). Here ξ_i is defined as the number of incoming messages at the sensor node, either generated by the node itself or the forwarded messages and ξ_o is defined as the number of outgoing messages. Such bursts of information usually create a short lived congestion inside the network [He et al., 2008]. Furthermore, when the overall network load is increased such that ReCAIT is not able to mitigate the congestion by dispersing the information to its neighbors, the long lived congestion across the network is observed. Once the information accumulates at the sensor node, it has to do something in order to relinquish the information load. Information accumulation is an indication that the next hop node along the path is not able to accept the information. It can be due to several reasons (1) the wireless link is congested (contention) (2) the buffer of next hop node is full and congestion arises due to buffer overflow and (3) the next hop node is unavailable, e.g., crashed due to energy depletion.

We first describe how ReCAIT approach proactively detects congestion inside the WSN. Next, we detail the congestion mitigation mechanisms of ReCAIT.

6.3.1 Proactive Congestion Detection

In order to provide proactive congestion control each sensor node in the WSN monitors the network conditions and the information rate across it. Each sensor node keeps an exponentially weighted moving average (EWMA) of $\xi_i(t)$ and $\xi_o(t)$ over a short time window T of the number of messages that it is transporting (Algorithm 5: lines 3-4), where α is a weight-factor ranging between $0 < \alpha < 1$. The EWMA approach avoids the wrong node decisions due to sudden or abrupt changes. ξ_i and ξ_o can be measured at each sensor node on a message by message basis. ReCAIT provides a generic and simple method to precisely measure the information rate at each intermediate sensor node using ξ_i and ξ_o. Based on this, the congestion factor (ς) can be defined

as

$$\varsigma = \mid \frac{\xi_o(t)}{\xi_i(t)} \mid \tag{6.7}$$

ς is an efficient and proactive indicator of the congestion since it requires only the count of incoming and outgoing messages. The existing approaches [Sankarasubramaniam et al., 2003; Wan et al., 2003; Wang et al., 2007a] detect congestion when it really happens based on some threshold on buffer occupancy or complex mechanism of computing timers for incoming and servicing of the messages. If at time t, $\varsigma < 1$, the sensor node detects the presence of congestion due to high information rate, i.e., number of incoming messages is higher than the outgoing messages. On the other hand $\varsigma > 1$ represents low information rate across the node and thus no congestion is observed.

Due to high information rate across the sensor nodes wireless link congestion builds up. We now present how ReCAIT copes with wireless link congestion.

6.3.2 Mitigating Wireless Link Congestion

In WSNs, when information rate increases, the message loss also increases due to the presence of channel contention. We refer to this as the wireless link congestion. Therefore, it is required to schedule the information transmission such that it does not interfere with transmissions of other sensor nodes in the neighborhood. In literature we find many MAC protocols [Langendoen, 2008], which also provide contention control. The major focus of MAC layer is on reduction of energy consumption to maximize the lifetime of the network and is unaware of application requirements. Therefore, ReCAIT provides an efficient reliability and application-aware mechanism to schedule message transmission across the nodes. To reduce the interference between messages, inter-node message scheduling takes into account the desired reliability of messages stored by the sensor nodes. Thus, the nodes having more messages with higher reliability requirements transmit the messages earlier. To enable this sensor nodes calculate the average reliability of buffered messages ($R_{q_{avg}}$) as follows

$$R_{q_{avg}} = \frac{\sum_{i=1}^{q_o} R_{h_{d_i}}}{q_o} \tag{6.8}$$

Each sensor node also piggybacks $R_{q_{avg}}$ when transporting the message. Upon snooping or receiving the message, Node Y compares its tuple ($\langle q_o, R_{q_{avg}} \rangle$) with the received message. Node Y will change its behavior only if its tuple is lower then the received node's tuple, i.e., its buffer occupancy and information reliability requirement is less. In this case Node Y

does not send any message during $\beta \cdot t_o$ time units, where β is waiting factor. β should be defined in such a way that the probability of all waiting nodes starting their transmissions simultaneously is reduced, and that higher-tuple nodes tend to wait for shorter time. We define β as follows

$$\beta = max(R_{q_{avg_X}}, R_{q_{avg_Y}}) + min(q_{o_Y}, q_{o_X}) + \gamma \tag{6.9}$$

where $0 < \gamma < 1$ is a drift and taken at random to avoid simultaneous transmission. It should be noted that the above scheduling starts when the sensor nodes detect the congestion (Section 6.3.1). ReCAIT efficiently tolerates the message loss due to contention by providing mechanism to efficiently schedule the message transmission. Next, we present how ReCAIT approach copes with the message loss due to buffer overflows caused by short lived congestion (Algorithm 5).

6.3.3 Mitigating Short Lived Congestion

We now present a solution for mitigating short lived congestion (Algorithm 5) which assures tunable reliability by adjusting the per hop desired reliability upon congestion detection and dispersing the information to the neighbor nodes. Once Node X locally detects the short lived congestion (Equation (6.7)), it disperses the information to the set of neighbor nodes, i.e., N_d,N_e and N_u in round robin fashion except the node from which it received the information (Algorithm 5: line 18). ReCAIT maintains a set of N_d, N_e as well as N_u for each sensor node sorted in the order of highest hop reliability across neighbors. More specifically, each Node X maintains the hop reliability $R_{hop_{(X,Y_i)}}$ and hop distance to the sink $h(Y_i)$ of each of its one hop neighbor Y_i (Algorithm 5: lines 14-17). By dispersing information from the point of congestion to the neighbor nodes assure that the congestion will not accumulate on the single path and provides the braided multiple paths. This braided effect is useful since information will converge to the optimal path [Ganesan et al., 2001] as soon as it bypasses the congestion spot in the network. The sensor node that detects the congestion determines the neighbor nodes in N_d and transports the next information to it (Algorithm 5: lines 20-22). Node X traverses the whole set and sends information to each neighbor one by one. If still the information rate is high, i.e., if congestion still persists and there are no more neighbors to choose from (i.e., $N_d = \emptyset$), nodes from N_e are selected to transport the information (Algorithm 5: lines 24-28). In the worst case if both sets are empty, the information is transmitted to the neighbors in N_u (Algorithm 5: lines 31-34). ReCAIT utilizes only the local knowledge to disperse the information to its neighbors. If Node X selects a

neighbor node in N_d it will not change the reliability assigned by the source node, i.e., R_{h_d} since the number of hops remains same for information to travel. If the neighbor belongs to N_e or N_u, Node X recalculates the desired hop reliability as follows:

$$R'_{h_d} = (\frac{R_d}{R_{h_d}})^{1/h(Y_i)} \tag{6.10}$$

Where R_{h_d} is the previously calculated reliability available from the received message and $h(Y_i)$ is the hop distance to the sink of the neighbor. If Node Y_i also experiences high information rate it follows the same procedure and sends the information to its neighbors. In this way, the information eventually bypasses the congestion area and starts flowing towards the sink.

It should be noted that to mitigate a short lived congestion we assume that the sensor nodes around the congestion area are not heavily loaded, i.e., the information flow is very low across them. By dispersing the information to neighbor nodes ReCAIT provides message loss tolerance against congestion. A sensor node keeps track of high information rate periodically (with time period T) and as soon as $\varsigma > 1$, the sensor node reverts back to default SP and sends information to its next hop node assigned by the underlying routing. Next we present Algorithm 6 which deals with the long lived congestion.

6.3.4 Mitigating Long Lived Congestion

Once the network load increases further such that a sensor node after dispersing the information to its neighbors is not able to alleviate the congestion, we say that a sensor node has detected long lived congestion. In such a case the only solution is to inform the source nodes to decrease the information rate such that the congestion can be alleviated. Our approach is to let sensor nodes keep track of buffer sizes q_{o_i} of their neighbors upon dispersing the information. When the buffer occupancy of all neighbor nodes is above some threshold (Q_{th}) a sensor node concludes that it can not disperse information further to its neighbors (Algorithm 6: lines 2-10). Unlike existing approaches [Ee and Bajcsy, 2004; Wan et al., 2003; Wang et al., 2006b], where they send explicit congestion notification immediately to source nodes to reduce the information rate, ReCAIT tries to alleviate congestion at each step during back propagation. Since each node is following the same procedure, ReCAIT does not require any explicit long lived congestion notification. If congestion is detected at certain hop ReCAIT enables the upstream hop to monitor the situation using Equation (6.7). Following this, the long lived congestion notification is implicitly back propagated to the source nodes. Once the source

Algorithm 5: Short Lived Congestion Control by ReCAIT

```
1  for each time interval T do
2      each node monitors the current ξ_i(t) and ξ_o(t);
3      ξ_i(t) = α · ξ_i(t) + (1 − α) · ξ_i(t − T);
4      ξ_o(t) = α · ξ_o(t) + (1 − α) · ξ_o(t − T);
5      ς = |(ξ_o(t)/ξ_i(t))|;
6      if ς < 1 then
7          organizeNeighbors();
8          disperseInfo();
9      end
10     else
11         transport(msg,Y_i,FALSE); \\Alg. (4)
12     end
13 end
14 function organizeNeighbors():
15 1-hop neighbors → N_d,N_e,N_u;
16 sort N_d,N_e,N_u according to max R_hop;
17 end function
18 function disperseInfo():
19 for each information in q_o do
20     if (N_d≠∅) then
21         select next Y_i ∈ N_d;
22         transport(msg,Y_i,TRUE);
23     end
24     else if (N_e≠∅) then
25         select next Y_i ∈ N_e;
26         calculate R'_{h_d} according to Equation (6.10);
27         msg.R_{h_d} ← R'_{h_d};
28         transport(msg,Y_i,TRUE);
29     end
30     else
31         select next Y_i ∈ N_u;
32         calculate R'_{h_d} according to Equation (6.10);
33         msg.R_{h_d} ← R'_{h_d};
34         transport(msg, Y_i, TRUE);
35     end
36 end
37  end function
```

node detects long lived congestion (Algorithm 6: lines 2-10) it reduces the information rate. We rely on existing work for rate regulation, where commonly

Additive Increase Multiplicative Decrease (AIMD) scheme is used. Once the source node detects congestion, multiplicative decrease is performed (Algorithm 6: lines 12-14). AIMD additively increases the information rate once congestion is mitigated (Algorithm 6: lines 18-19).

Algorithm 6: Long Lived Congestion Control by ReCAIT

```
1  if forwarding node then
2      if (∀ q_o = Q_th) then
3          wait for time interval T;
4          for each neighbor node do
5              if q_oi < Q_th then
6                  transport(msg,Y_i,TRUE); \\Alg. (4)
7              end
8          end
9      end
10 end
11 if source node then
12     if (∀ q_o = Q) and (ς < 1) then
13         infoRate[N_d,N_e,N_u] *=decInfoRate[N_d,N_e,N_u]; \\multiplicative
           decrease
14     end
15     else if (∀ q_o ≠ Q) and (ς < 1) then
16         disperseInfo(); \\Alg. (5)
17     end
18     else if (∀ q_o ≠ Q) and (ς > 1) then
19         infoRate[SP] += incInfoRate[SP]; \\additive increase
20     end
21 end
```

The unavailability of sensor nodes is inherently tolerated by ReCAIT. At transport layer abstraction node failure is similar to a transient failure. Practically, the unavailability of a sensor node is equivalent to the link loss scenario as the underlying routing protocol is responsible to maintain the route. While the routing protocol repairs the paths, ReCAIT may perceive higher information rate across the node which will consequently results in congestion. In this case ReCAIT splits the information across the neighbor nodes. Once the path is repaired ReCAIT reverts back to its normal operation.

6.4 Performance Evaluation

In order to evaluate our approach we first describe an evaluation scenario and the simulation settings. Next, we present and discuss our simulation results.

6.4.1 Methodology and Simulation Settings

We consider a scenario where the phenomenon of interest corresponds to spatio-temporal bursts of information. Only the sensor nodes covered by the spatial phenomena generate information and transport them along SP towards the sink. This incurs a substantial congestion on the nodes along the path. Before a phenomenon occurs, the information rate is very low and the network does not experience congestion.

In order to simulate the scenario, we assume 100 sensor nodes (until and unless specified) in an area of 60x60 $unit^2$ with n x n grid topology. The distance between two nodes is 5 unit. A grid topology is chosen to emulate uniformly dense deployments but is not required by our algorithms. The sink is located at one corner of the area. Four randomly selected nodes in the opposite corner to the sink generate atomic information. This placement of the sources in our simulations was selected to get a sufficient number of hops to the sink. In a large deployment of hundreds of nodes, these sources need not be at the corner of the deployment. Results were recorded when the system reached a steady state. For every simulation run the node generate 50 messages to be transported towards the sink. The size of the message is 29 bytes and each sensor node has buffer size of 36. For MAC we have used default CSMA-based implementation. We select multiplicative decrease cutoff value of 0.85 [Popa et al., 2006]. In order to maintain R_{hop}, a sensor node keeps track of the link quality between its neighbor nodes using EWMA approach. A sensor node keeps track of link quality in terms of bit error probability (BEP) between itself and its neighboring nodes upon reception of a message or when it snoop the channel for IACK. At a node, other local parameters such as t_o and t'_o are calculated similarly using EWMA approach. A typical value of $\alpha, \gamma = 0.1$ [Wang et al., 2007a] is used in the simulations.

We compared the ReCAIT with its variants, i.e., ReCAIT with no congestion control (ReCAIT-NoCC) and ReCAIT with short lived congestion control (ReCAIT-SLCC), Modified MMSPEED protocol (MMP) and RBC. ReCAIT-NoCC exploits only the temporal redundancy, i.e., adaptive retransmissions and does not provide congestion control. ReCAIT-SLCC disperses the information upon detection of short lived congestion, whereas ReCAIT is the combination of short and long lived congestion. As the code for MMSPEED is not available for TOSSIM, we implemented its reliability module,

i.e, MMP. For fair comparison we used CSMA/CA without RTS/CTS as suggested by the authors of MMSPEED. We compared ReCAIT with MMP in order to observe the impact of on-demand and always available multiple paths. We also compared ReCAIT with RBC as it specifically provides reliable information transport in presence of high information rates. For underlying routing we modified the Logical Grid Routing (LGR) [Choi et al., 2006] protocol. LGR creates a spanning tree rooted at the sink and periodically exchanges topology information to maintain the spanning tree. Our modified LGR provides a node with the list of one hop neighbors.

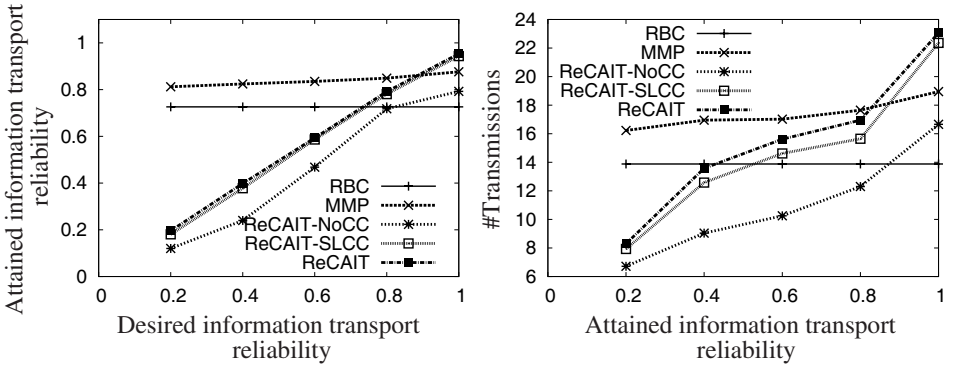
6.4.2 Simulation Results

Now we present our simulation results for different studies that we conducted, i.e., impact of tunable reliability, information rates, network conditions, number of nodes and number of information flows.

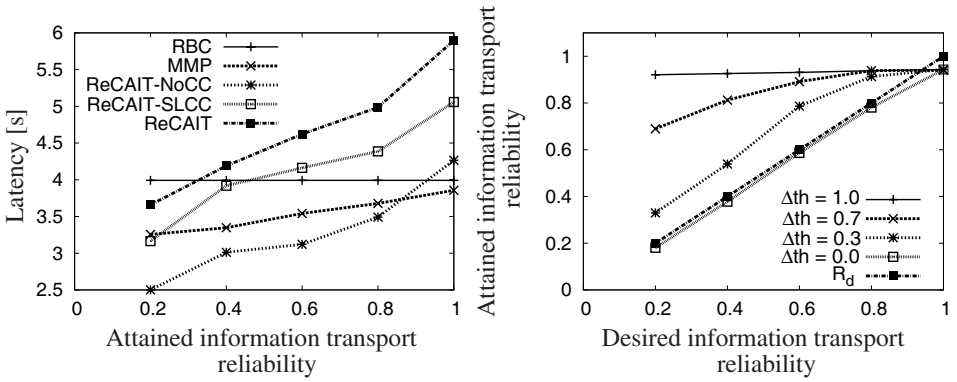
Tunable Reliability of Information Transport

First, we evaluate the performance of ReCAIT for tunable application requirements. In this study the sensor nodes generate the information at 10 messages per second (msgs/s) and transport them towards the sink. Figure 6.1 (a) shows the tunability of the different protocols. Since RBC does not provide tunability it achieves a constant reliability, which is less than 1. Though RBC is developed specifically to cope with the bursty nature of information, it can not handle high information rate. MMP also shows almost constant behavior since it always tries to provide higher reliability than required. ReCAIT-NoCC on the other hand tries to fulfill the tunability requirements but starts dropping information along the path when congestion builds up. ReCAIT-SLCC fulfills the tunable reliability requirements despite the high information rate by dispersing the information on different neighbor nodes. This is also evident from Figure 6.1 (b) where ReCAIT-SLCC shows more transmissions compared to ReCAIT-NoCC. This behavior validates the impact of Algorithm 5 where ReCAIT-SLCC adapts to high information rate and disperses information to neighbors resulting in higher number of transmissions. MMP and RBC always have higher number of transmissions due to the fact that MMP sends information on multiple paths and RBC retransmits upon loss of information. The number of transmissions for ReCAIT-SLCC and ReCAIT remains low for application reliability 0.2 to 0.8, since it adapts #ret, opportunistically suppresses and utilizes hybrid ACK with respect to application requirements and network conditions. For reliability of 1.0 ReCAIT-SLCC and ReCAIT have higher number of transmissions

which corresponds directly to the higher reliability achieved than any other protocol. Figure 6.1 (c) shows the timeliness tradeoff for different protocols. The local timer management accurately estimates the retransmission timeouts to minimize the number of transmissions. Local timer management approach shows conservative behavior since its latency is higher compared to other protocols. For ReCAIT-NoCC the timeliness remains low, which corresponds to the low reliability attained. MMP shows lower latency than ReCAIT due to use of multiple paths. This can be beneficial in some cases, i.e., to real time applications, but comes at the expense of higher number of transmissions. Figure 6.1 (d) shows how ReCAIT behaves depending on Δ_{th}. With increasing Δ_{th} we observe that the attained reliability is proportionally increased according to desired reliability. This behavior of Δ_{th} confirms that the information transport reliability is always between R_d and $(R_d + \Delta_{th})$. $\Delta_{th} = 1.0$ leads to the fact that ReCAIT will not suppress the messages and always transport them towards the next hop and behaves similar to MMP and RBC, i.e., always provide higher reliability.



(a) Information transport reliability (b) Information transport efficiency

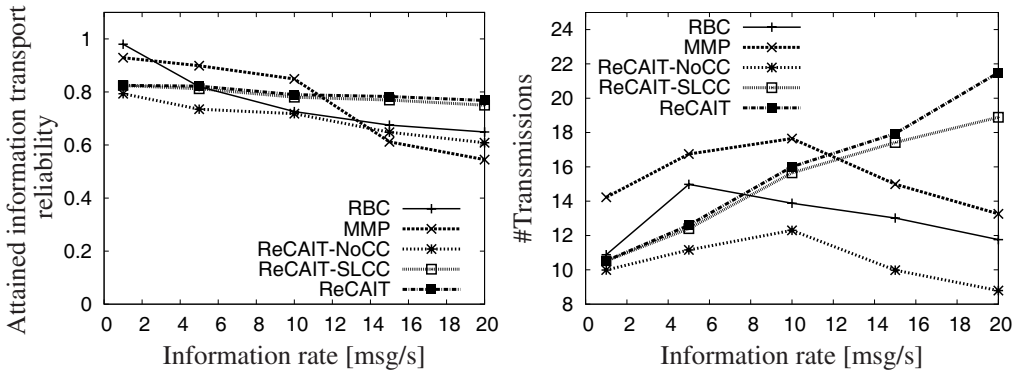


(c) Information transport timeliness (d) Impact of Δ_{th}

Figure 6.1: Tunable reliability of information transport

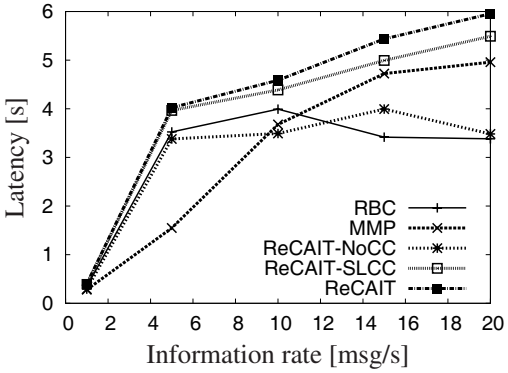
Adaptation to Information Rate

As information rate impacts the congestion level, now we study how the different protocols adapt to increasing information rates. In this study we assume that the application requires 0.8 reliability. Figure 6.2 (a) shows that the ReCAIT-SLCC and ReCAIT adapt to the information rate appropriately than all other protocols. At low information rate, i.e., when there is less congestion RBC and MMP provide higher reliability than required and ReCAIT adapts to provide the required reliability and probabilistically suppress the information. Similarly, ReCAIT-NoCC also provides desired reliability at low information rate. However, as soon as the information rate is increased MMP, ReCAIT-NoCC and RBC degrade, whereas ReCAIT-SLCC and ReCAIT maintain the desired application reliability owing to adaptive spatial reuse. The reliability of MMP decreases because of increasing information flow on multiple paths which result in high collisions and dropping of messages. RBC also fails to avoid congestion due to high information rate



(a) Information transport reliability

(b) Information transport efficiency



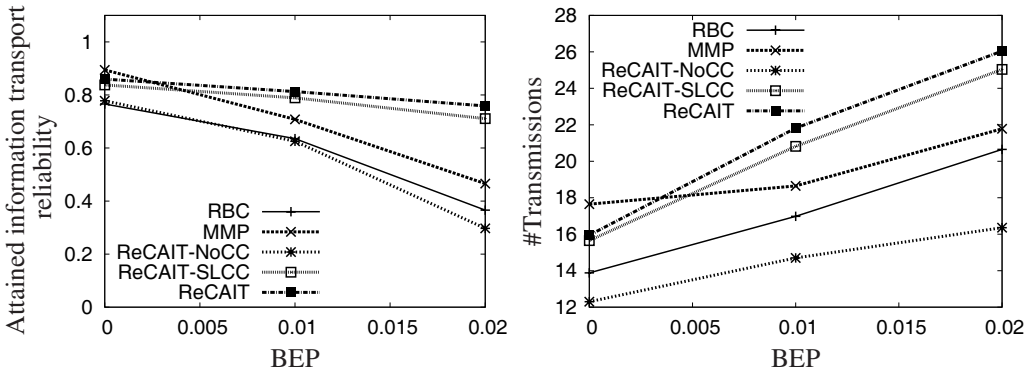
(c) Information transport timeliness

Figure 6.2: Adaptation to information rate ($R_d = 0.8$)

and start dropping the messages. Figure 6.2 (b) shows the increase of transmissions for ReCAIT-SLCC and ReCAIT as it adapts to utilize the multiple paths. It is noteworthy that the number of transmissions for all other protocols decreases with the increasing information rate. This is due to the fact that the protocols drop the information due to congestion. Similar effect can be observed for timeliness in Figure 6.2 (c) where for RBC, MMP and ReCAIT-NoCC latency decreases which is directly proportional to reliability and dropped information. Whereas, ReCAIT-SLCC and ReCAIT follow split paths and local timer management resulting in high latency. It is also interesting to observe that the latency of MMP increases with high information rate. MMP utilizes more paths due to less reliability across hops (more collisions) which results in longer paths.

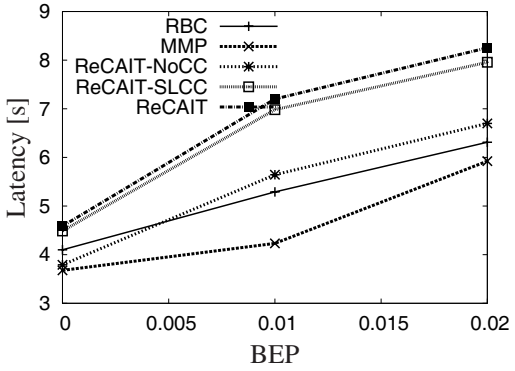
Adaptation to Network Conditions

We now investigate the impact of network perturbations. We consider an



(a) Information transport reliability

(b) Information transport efficiency



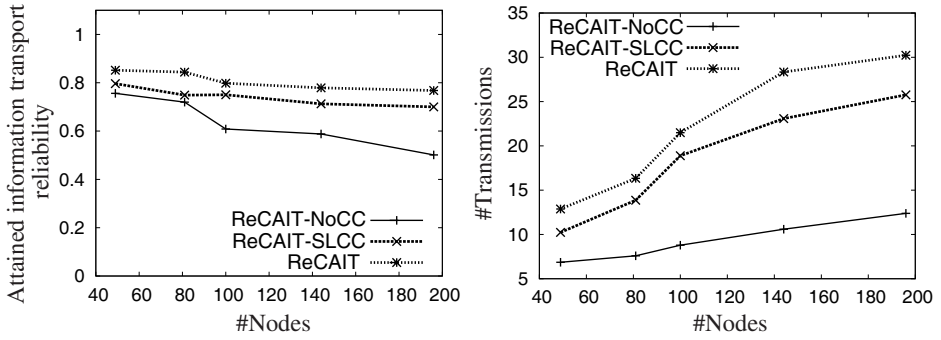
(c) Information transport timeliness

Figure 6.3: Adaptation to network conditions ($R_d = 0.8$)

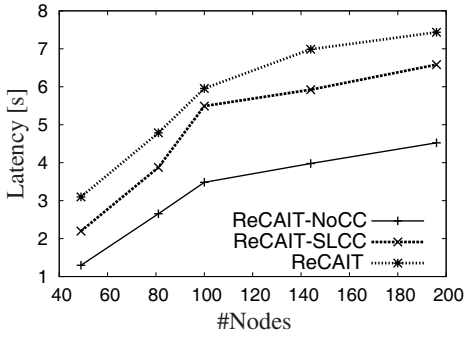
information rate of 10 msg/s and $R_d = 0.8$. Figure 6.3 (a) shows ReCAIT-SLCC and ReCAIT effectively adapts to wireless link perturbations due to the fact that ReCAIT utilizes the adaptive retransmissions and splits the information to multiple neighbors upon congestion. On the other hand, RBC utilizes fixed number of retransmissions and drops the information once congestion is encountered. Similarly, ReCAIT-NoCC and MMP also drop messages and do not provide the required information transport reliability as BEP increases. Figure 6.3 (b) - (c) confirms the behavior with growing number of transmissions and timeliness for ReCAIT-SLCC and ReCAIT. We also observe that at BEP 0.0 ReCAIT-NoCC performs better than MMP and RBC with respect to number of transmission and latency, since it adapts to the application requirements. At higher BEP the number of transmissions increases due to higher number of retransmissions resulting in higher latency.

Adaptation to Network Size

In this study we show the scalability of ReCAIT for various number of sensor nodes. The information rate is 20 msg/s and $R_d = 0.8$. We vary the number



(a) Information transport reliability (b) Information transport efficiency



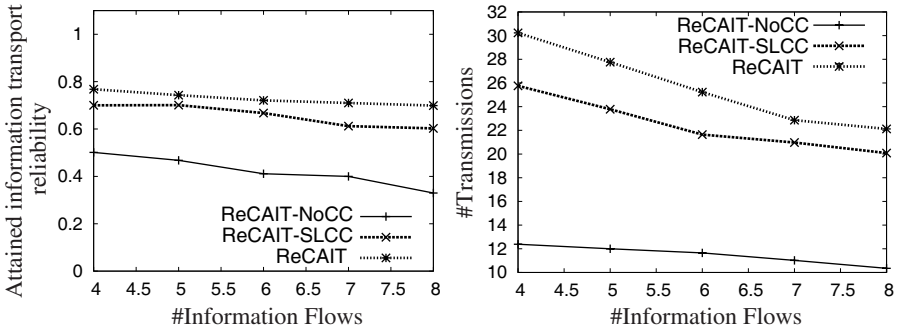
(c) Information transport timeliness

Figure 6.4: Adaptation to network size ($R_d = 0.8$)

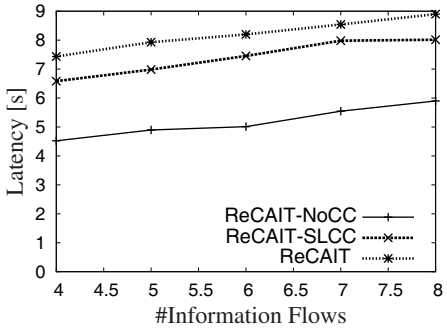
of sensor nodes between 49, 81, 100, 141 and 196. Figure 6.4 (a) depicts the attained reliability by ReCAIT and its variants. ReCAIT-NoCC deviates and provides less reliability when the number of sensor nodes increases. ReCAIT always provides application specific reliability despite increasing amount of sensor nodes by adapting localized mechanisms. We also observe that for less number of sensor nodes, i.e., less number of hops, ReCAIT attains application specific reliability by efficiently mitigating link congestion and using robust scheduling among the neighbor nodes. Figure 6.4 (b) shows obvious increase in number of transmissions. For ReCAIT-NoCC the number of transmissions is relatively low because upon congestion messages are dropped which directly affects the attained reliability. Figure 6.4 (c) illustrates the timeliness of the protocols. The trends are similar and the latency of all protocols increases with the number of sensor nodes. These results confirm that the localized mechanisms of ReCAIT make it a scalable solution.

Adaptation to Number of Information Flows

Figure 6.5 presents the performance result for 200 nodes and the application



(a) Information transport reliability (b) Information transport efficiency



(c) Information transport timeliness

Figure 6.5: Adaptation to number of concurrent information flows ($R_d = 0.8$)

reliability requirement of 0.8. ReCAIT and ReCAIT-SLCC maintain the application specific reliability (Figure 6.5 (a)) but we observe in Figure 6.5 (b) that the number of transmissions decreases as the network becomes congested regardless of the mechanism used and the information rate is decreased. Due to congestion both at link and buffer, the latency is also increased (Figure 6.5 (c)).

6.5 Chapter Summary

In this chapter, we proposed a tunable reliability approach with congestion awareness for information transport termed as ReCAIT. ReCAIT provides the desired application reliability despite evolving network conditions by adaptive retransmissions and by suppressing the unnecessary transmissions. Reliability of information transport is achieved by hybrid ACK mechanism aided by retransmission timer management. ReCAIT efficiently monitors the information flow and adapts between single path and braided multiple paths in order to alleviate congestion and to maintain the desired application reliability. If congestion persists ReCAIT utilizes its long lived congestion mitigation mechanism to alleviate it. The simulation results confirm the capability of the ReCAIT approach to tune according to the application requirements and adaptability to information rate, changing network conditions and network traffic. The results also confirm that the performance of the ReCAIT approach is not affected by the scaling of the network.

Chapter 7

Evaluation of the Generic Information Transport Framework

In order to evaluate the Generic Information Transport (GIT) Framework as discussed in Chapter 4, 5 and 6, we first describe the evaluation methodology and simulation settings. Next, we present our simulation results corresponding to different studies we conducted. Chapter 5 and 6 individually validated the different modules of GIT. In this chapter we observe the combined effect of all the modules and see how GIT performs in various conditions. For this we conduct various studies to explore the full functionality of GIT.

7.1 Methodology and Simulation Settings

To observe the tunability of GIT and how it manages different types of information, we simulated the following scenario. We considered atomic (AI), redundant atomic (RAI) and composite information (CI) for transportation. The application requires $R_d = 0.7$ in the first phase. Each type of information is generated every 10 seconds and transported towards the sink. After 5 mins the application tune its requirement, i.e., $R_d = 0.5$. To simulate the evolving application requirement scenario, again after 5 mins the application requirements are changed to $R_d = 0.8$. The above scenario is representative for various situations inside the network. First, it represents evolving application requirements. Second, when many sensor nodes send information towards the sink it leads to evolving network conditions, i.e., increased collisions and contention.

In order to observe the GIT adaptation to evolving network conditions

the following scenario is considered. We assume AI to be transported to the sink. The application requirement is 100% throughout the scenario. This also shows the GIT's performance for high reliability requirements. The AI is generated every 10 seconds and transported towards the sink. in first phase of the simulation the network conditions are kept good , i.e., BEP = 0.0. After 5 mins the network condition is changed by changing the BEP to 0.01. To simulate the dynamic network conditions scenario, again after 5 mins the network condition is changed (BEP = 0.02).

In another simulation setting we kept the application requirements unvarying ($R_d = 0.8$) and change the information rate to monitor GIT's performance for various congestion scenarios.

In order to simulate the scenario, we deployed 225 sensor nodes in an area of 75×75 $unit^2$ with 15×15 grid topology. The distance between two neighboring nodes is 5 units. For atomic information one node is randomly chosen from the opposite corner of the sink. For redundant atomic information, 20 nodes are selected randomly close to each other within the radius of 15 units. For composite information, nodes on the periphery of redundant atomic information choose themselves for information transport. Both redundant atomic information and composite information are generated in the opposite corner of sink. The size of the message is 29 bytes and each sensor node has buffer size of 36 messages.

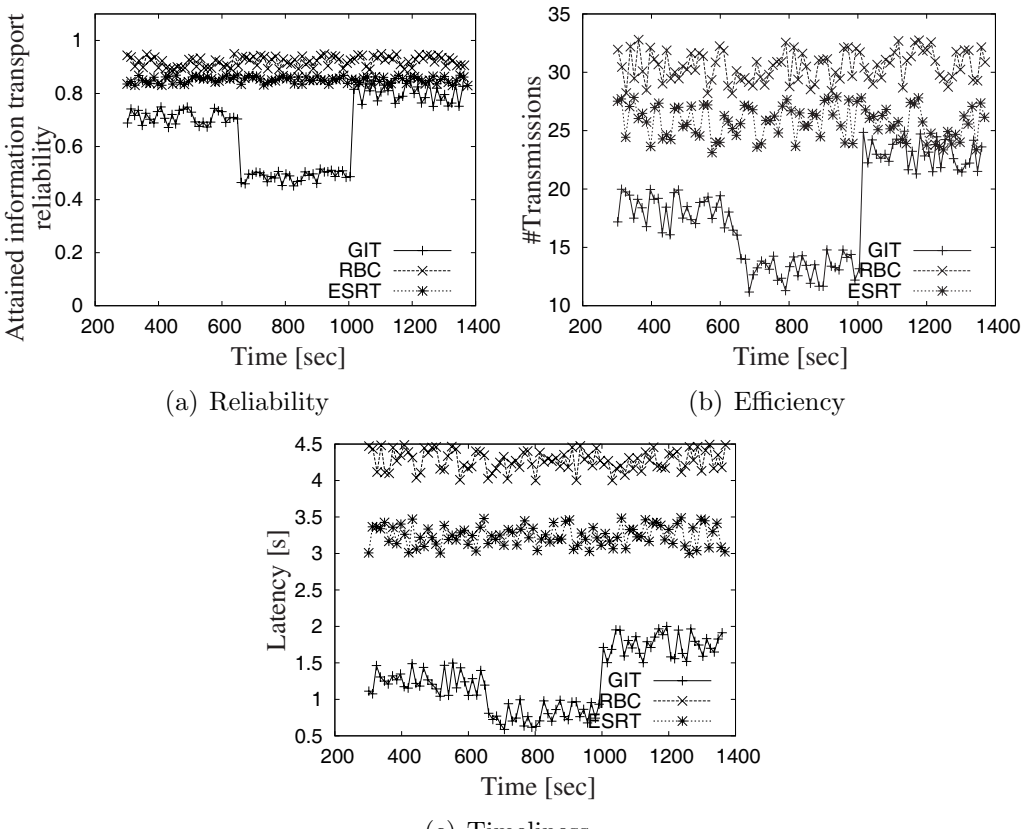
We used representative protocols from the existing literature as discussed in Chapter 3 and compared them with the GIT framework. We selected reliable bursty convergecast (RBC) [Zhang et al., 2005], which provides only reliability and event to sink reliable transport (ESRT) [Sankarasubramaniam et al., 2003], which provides both reliability and congestion. The source code of RBC is available for the mica2 mote platform, consequently we ported the RBC code to execute under the TOSSIM environment. The code for ESRT is not available thus, we implement ESRT in TOSSIM. As for routing the messages, RBC uses by default logical grid routing (LGR) [Choi et al., 2006] protocol, we have chosen LGR for routing the messages for fair comparison.

7.2 Simulation Results

Now we present our simulation results for different studies that we conducted, i.e., impact of tunable reliability, network conditions, information rate. We further analyze the impact of number of information nodes on redundant atomic and composite information.

7.2.1 Tunable Reliability of GIT

First, we consider the varying application requirements scenario. Figure 7.1 depicts the tunability of atomic information transport. The reliability attained by the GIT and other protocols is shown in Figure 7.1 (a). As RBC and ESRT do not provide tunability aspects, their attained reliability is steady over time. GIT supports tunable behavior and copes with the evolving application requirements. We observe that GIT always fulfills the application requirements (±3%). The reliability attained by the ESRT is lower than RBC since it does not utilize any message loss recovery mechanism. RBC reliability remains higher which is in contradiction to application requirements and waste critical resources by having more transmissions. Figure 7.1 (b) shows that GIT is efficient and uses fewer transmissions and adapts them according to application requirements owing to adaptive transmissions mechanism by TAM. ESRT shows fewer number of transmissions compared to RBC because ESRT does not employ retransmissions to recover information loss, resulting



(a) Reliability

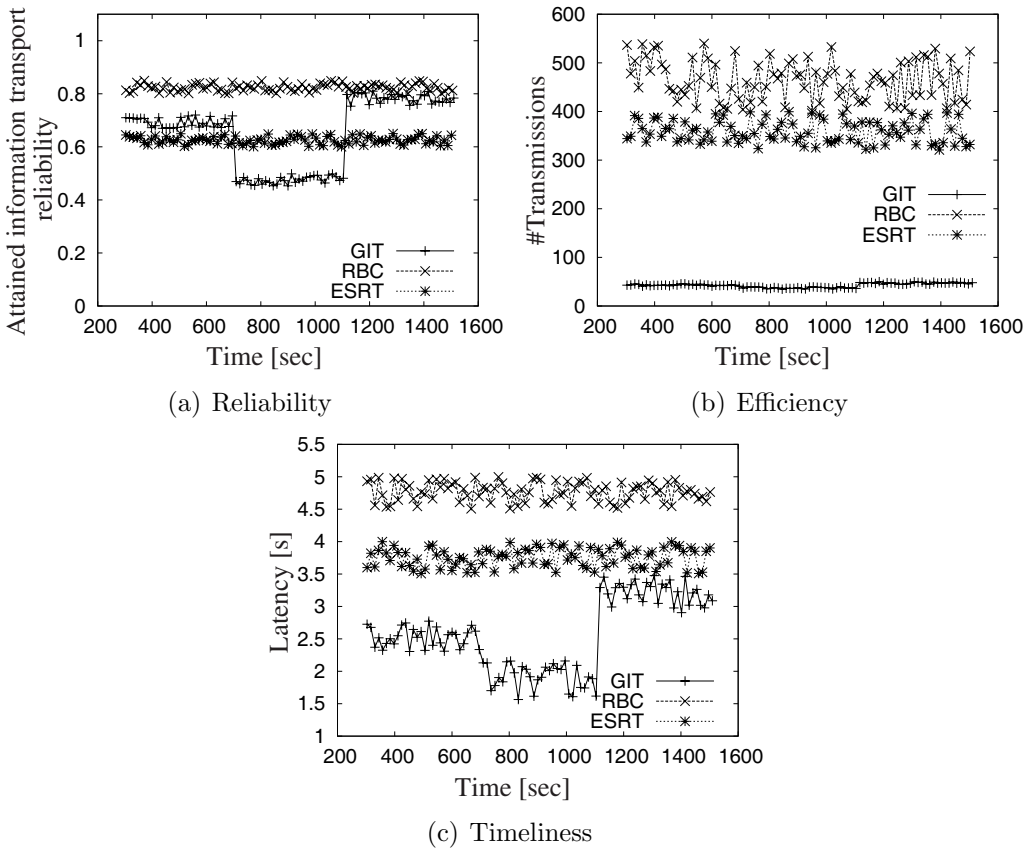
(b) Efficiency

(c) Timeliness

Figure 7.1: Tunability of atomic information

in low reliability as well. Figure 7.1 (c) shows the timeliness tradeoff of different protocols. GIT latency remains lower than that of RBC and ESRT due to efficient transport mechanisms which lower the probability of retransmissions thus, reducing the latency. ESRT and RBC as they always send information without caring for application requirements. Therefore, information is sent across the network every time resulting in contention leading to high latency.

Figure 7.2 shows the adaptation to application requirements for redundant atomic information. GIT adapts according to the application requirements and provides tunable reliability (Figure 7.2 (a)). The reliability attained by ESRT is lower than GIT and RBC because of message loss due to sudden bursts of information. Similarly RBC reliability also decreases but it responds better than ESRT due to its fixed number of retransmissions. We observe a tremendous benefit of GIT in terms of efficiency (Figure 7.2 (b)). The number of transmissions is reduced 4-5 times. This is achieved by GIT due to information awareness and the mechanisms utilized to reduce the re-



(a) Reliability

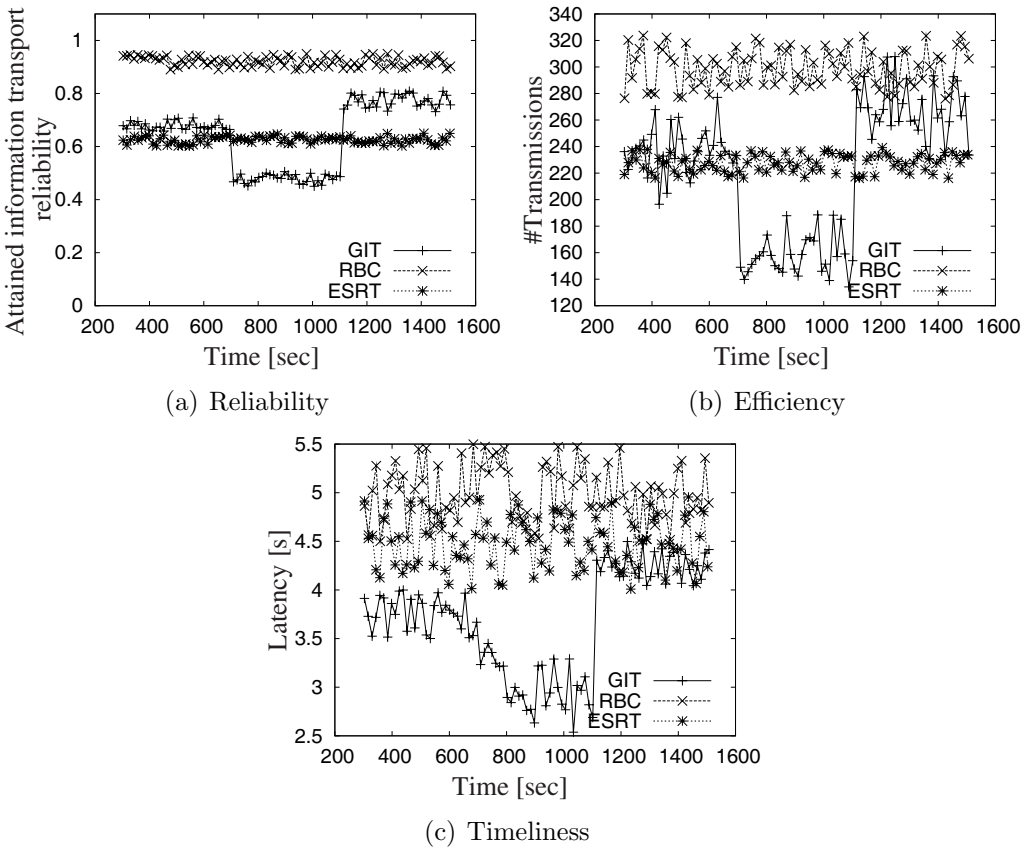
(b) Efficiency

(c) Timeliness

Figure 7.2: Tunability of redundant atomic information

dundant information. As ESRT and RBC cannot distinguish between the transported information, they result in higher number of transmissions. Figure 7.2 (c) shows the latency of GIT remains lower than ESRT and RBC because when the burst of information is generated by 20 nodes, RBC and ESRT have to cope with contention and retransmission. Whereas, GIT utilize efficient techniques as discussed in Section 4.3, which reduce number of nodes to contend, thus, resulting in low timeliness.

Figure 7.3 depicts the tunability of composite information. For composite information GIT also provides tunable reliability (Figure 7.3 (a)). In Figure 7.3 (b) we observe that at higher application requirement (i.e., 0.7 and 0.8) the number of transmissions of GIT is comparable to ESRT and RBC. The number of transmissions is directly proportional to the higher reliability requirement of the application. Furthermore, as multiple information flows start to flow towards the sink, congestion results. Here GIT adapts by splitting paths resulting in slightly higher number of transmissions. This is



(a) Reliability

(b) Efficiency

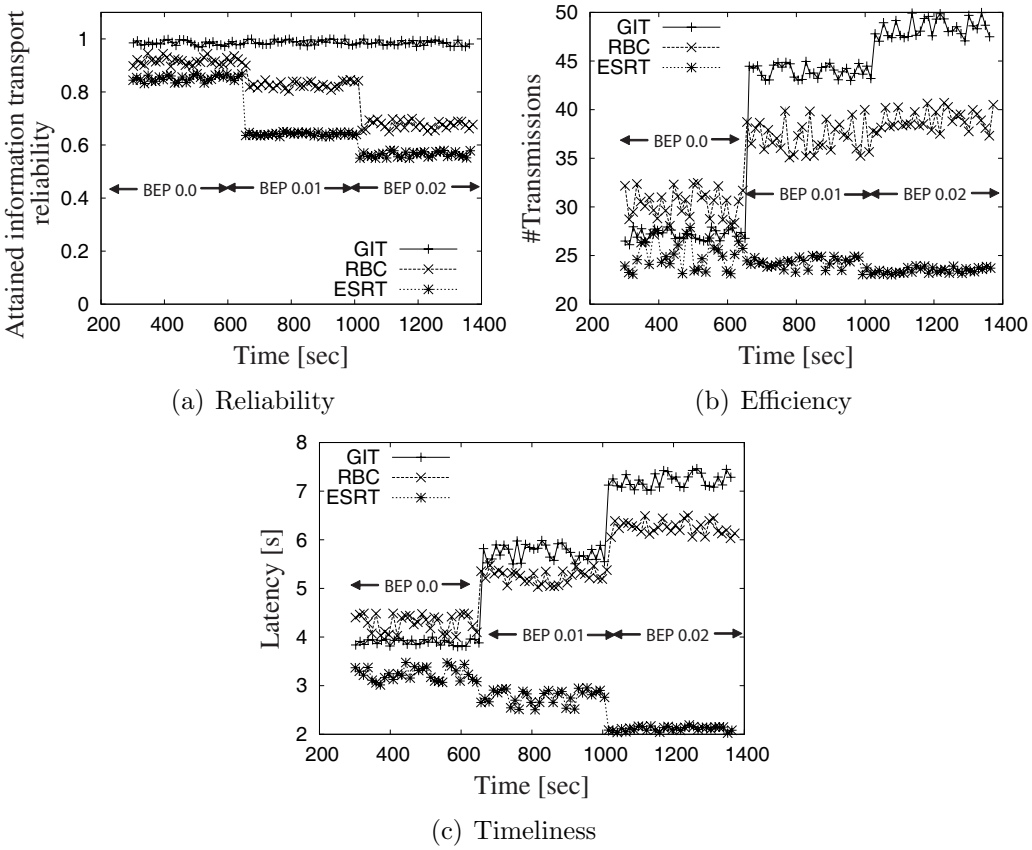
(c) Timeliness

Figure 7.3: Tunability of composite information

also because the sensor nodes selection is directly related to the application requirements. Therefore, at higher reliability requirements more nodes are selected resulting in short lived congestion. The timeliness of GIT also increases with higher application requirements (Figure 7.3 (c)) due to splited paths where information follows slightly longer paths.

7.2.2 Adaptation of GIT to Network Conditions

In this scenario we change the BEP instead of application requirements. This study provides insights into how the different solutions adapt according to the evolving network conditions. This scenario further provides imminent view on GIT's information transport when application requires 100% reliability. Figure 7.4 (a) presents results of attained reliability for dynamic network conditions. It is evident that GIT adapts according to the application requirements and always provides close to 100% reliability. RBC and



(a) Reliability

(b) Efficiency

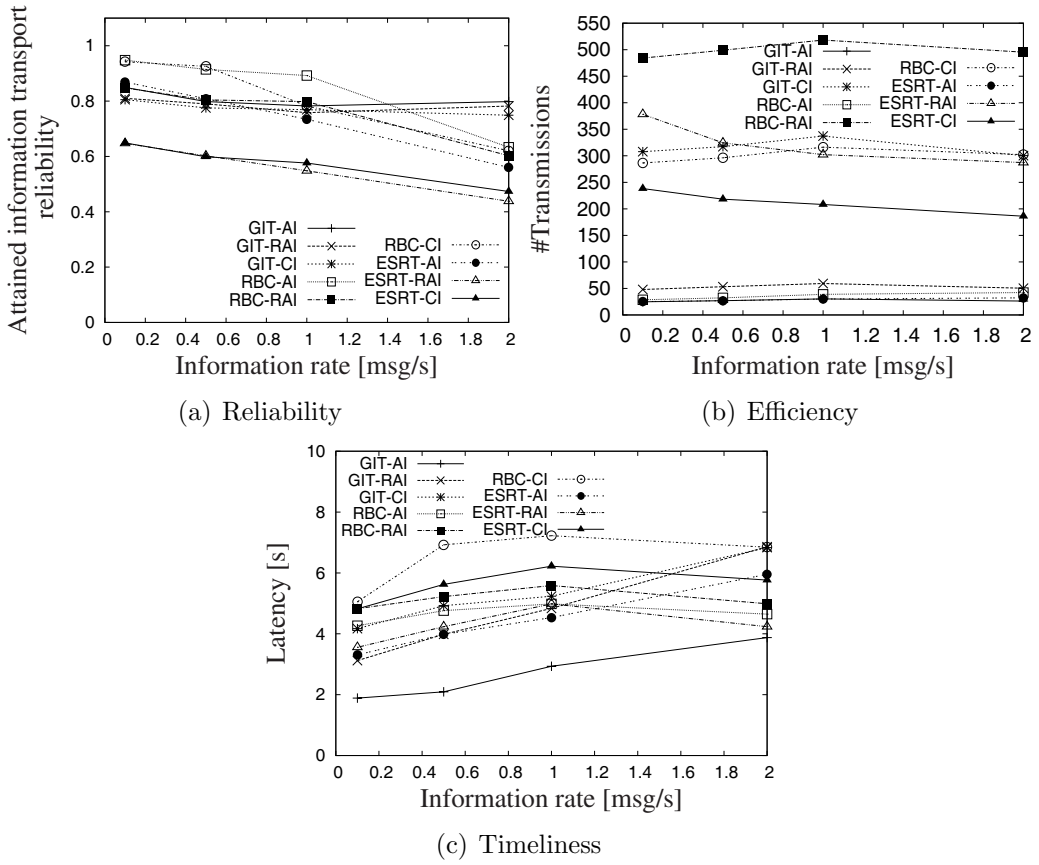
(c) Timeliness

Figure 7.4: Adaptation to network conditions (R_d= 1.0)

ESRT are not able to cope with the dynamic network conditions and the attained reliability is decreased. GIT maintains the desired reliability by using adaptive retransmissions and hybrid acknowledgement mechanism. When the network condition is good, i.e., BEP = 0.0, we observe that the number of transmissions are lower than RBC showing that the adaptive mechanisms by GIT provide high reliability efficiently (Figure 7.4 (b)). As the network conditions are evolving (BEP = 0.01, BEP = 0.02) the GIT adapts the number of retransmissions accordingly to maintain desired reliability resulting in higher number of transmissions compared to RBC and ESRT. However, the number of transmissions for ESRT decreases with the increasing BEP, since there is no information loss recovery mechanism. On the other hand, RBC's number of transmissions are bit increased with increasing BEP but not able to maintain the application specified reliability. Figure 7.4 (c) shows the latency tradeoff of GIT, RBC and ESRT. We observe that the latency of GIT increases with the evolving network conditions. There is a tradeoff between attained reliability, number of transmissions and latency. To maintain the desired reliability GIT utilizes more transmissions resulting in high latency, whereas ESRT and RBC provide less reliability corresponding to less transmissions and low latency.

7.2.3 Adaptation of GIT to Information Rate

We now consider a second scenario, where we assume $R_d = 0.8$ and a varying information rate. Figure 7.5 (a) depicts the GIT tunability to fulfill desired application requirements for varying information rate of different types of information. Figure 7.5 (a) depicts that GIT always provide reliability close to the application requirements. With high information rate (2 msgs/sec) RBC and ESRT are not able to cope due to collisions and congestion. While at low information rate RBC and ESRT provide high reliability. With increasing information rate congestion start to build and GIT efficiently handles the situation as shown in Figure 7.5 (b). We observe that for composite information at 1 msg/sec GIT utilizes more transmissions owing to split path mechanism used to avoid short lived congestion. When the information rate is further increased, the number of transmissions is lower due to decreased information rate as done by GIT to handle long lived congestion. For other types of information GIT also efficiently adapts transmissions. It is noteworthy that the number of transmissions for RBC and ESRT decreases with the increasing information rate. This is due to the fact that the protocols start dropping the information due to congestion. Similar effect can be viewed for timeliness in Figure 7.5 (c), where for RBC and ESRT latency decreases which is directly proportional to reliability and dropped information. GIT



(a) Reliability

(b) Efficiency

(c) Timeliness

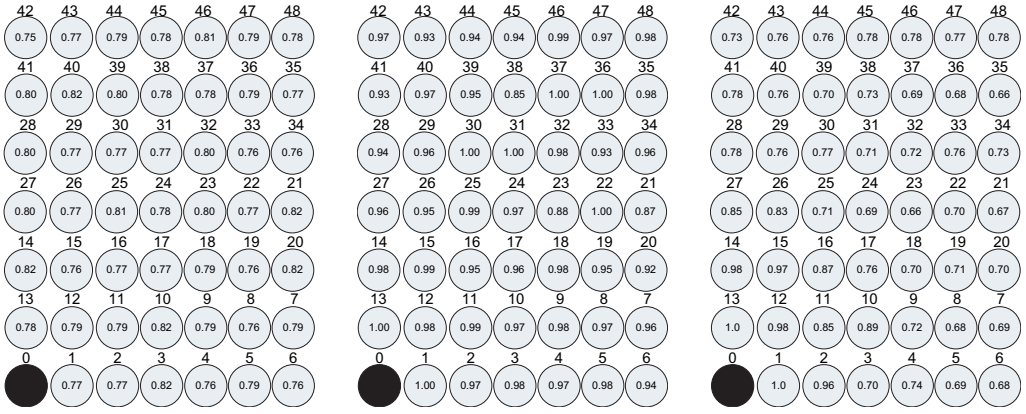
Figure 7.5: Adaptation to information rate ($R_d = 0.8$)

follows congestion control mechanisms and local timer management which results in slightly increased latency as information rate increases.

7.2.4 Reliability Attained by All Sensor Nodes

In this study we observe the GIT performance for all sensor nodes. Each sensor node generates atomic information every minute. This scenario corresponds to a monitoring application where the application is interested in gathering the environmental data to be available every minute. We consider 50 sensor nodes in the grid formation as in Figure 7.6 (a) and application requires 80% information transport reliability.

Figure 7.6 (a) depicts GIT capability to provide application specific reliability for all sensor nodes. On the other hand, RBC always provides high reliability and almost all information entities are received by the sink. Contrary, for ESRT we observe that nodes which are near to the sink have high



(a) GIT (b) RBC (c) ESRT

Figure 7.6: Reliability attained by all sensor nodes ($R_d = 0.8$)

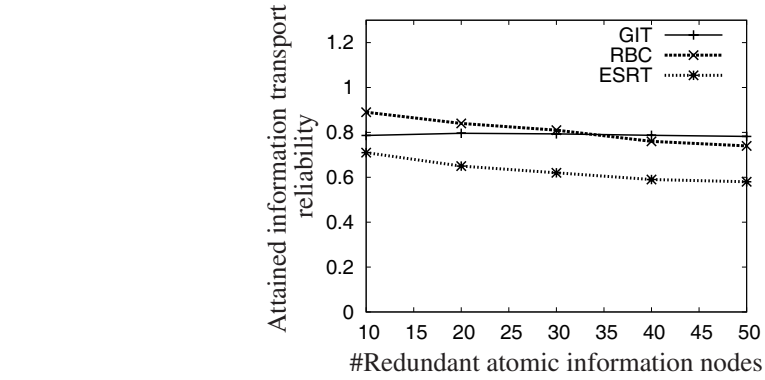
reliability and as the number of hops increases the transport reliability of the nodes is decreased Figure 7.6 (c). This study confirms the scalability of GIT and its applicability when all sensor nodes send the information to the sink.

7.2.5 Analysis of Redundant Atomic Information

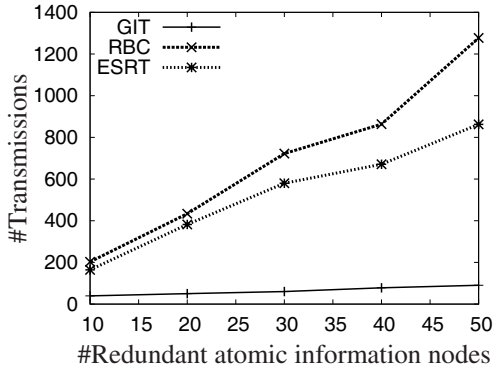
Figure 7.7 depicts the impact of number of information nodes on the redundant atomic information. Figure 7.7 (a) shows that GIT adapts according to application requirements and always provides 80% reliability. Although RBC and ESRT are intended to provide always high reliability, they are not able to attain it. When many sensor nodes start sending the information to the sink RBC and ESRT are not able to cope with the resulting collisions. GIT's efficient mechanism to manage the information, avoid the contention and collisions provides application specific reliability with lower number of transmissions (Figure 7.7 (b)). The number of transmissions directly impacts the latency of the approaches. Figure 7.7 (c) provide insights on the latency achieved by GIT compared to other solutions. We observe that GIT latency is always low compared to RBC and ESRT owing to lower number of transmissions and selection of information node in a proficient manner. Similar trend is maintained by GIT as the number of information nodes is increased, i.e., low latency.

7.2.6 Analysis of Composite Information

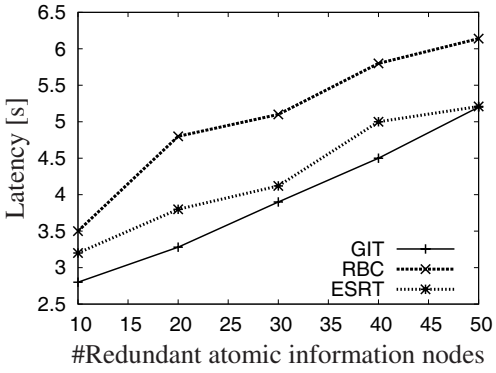
Figure 7.8 depicts the impact of information nodes for composite information. In this scenario 0.8 application requirement for information transport



(a) Reliability



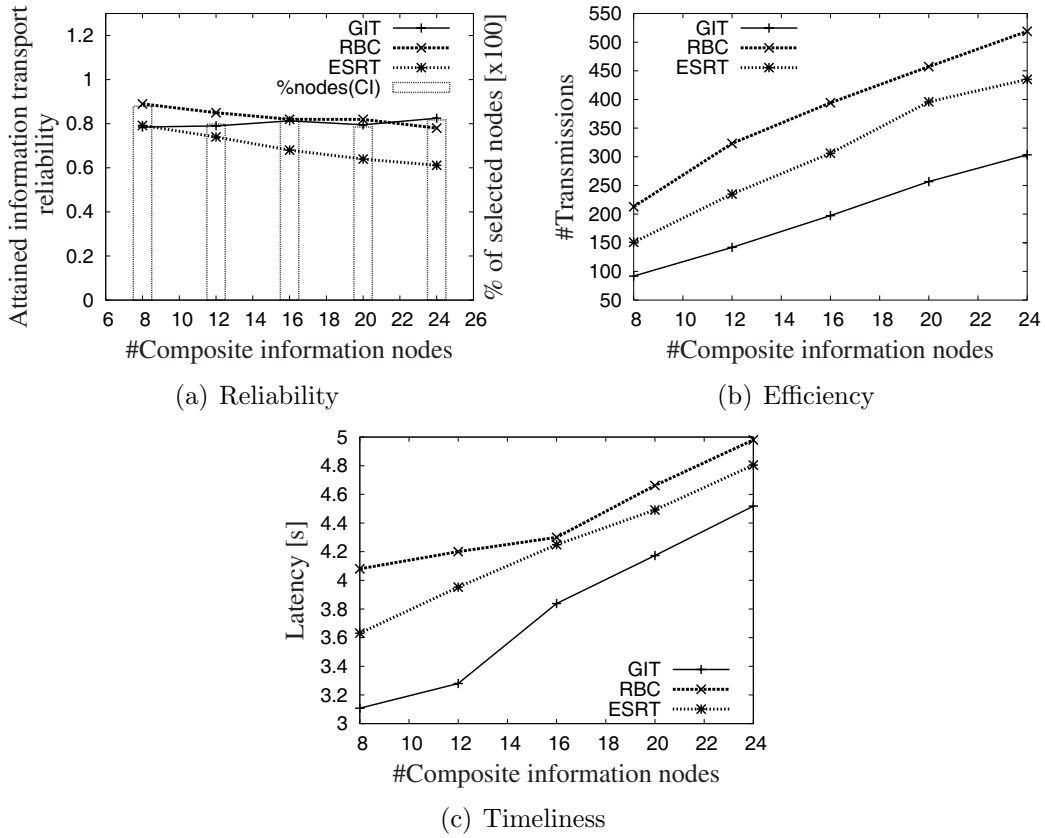
(b) Efficiency



(c) Timeliness

Figure 7.7: Impact of number of information nodes on redundant atomic information ($R_d = 0.8$)

is considered. Figure 7.8 (a) depicts the reliability of composite information. GIT adapts according to the type of information and selects the information nodes for information transport. As the number of nodes increases the reliability is maintained by GIT. RBC reliability gradually decreases with increase in number of nodes because of higher number of collisions near the information area. On the other hand, RBC reliability is higher than the ESRT due to its fixed number of retransmissions. For ESRT if the information entity is lost, it is lost forever as there is no recovery mechanism enabled by ESRT. For composite information the number of sensor nodes is unknown therefore, GIT randomly select them (Algorithm 2) and all selected nodes have to transport the information. With the increase in number of nodes their selection probability also increases, thus resulting in higher number of transmissions for GIT (Figure 7.8 (b)). The number of transmissions for RBC and ESRT is always higher than the GIT (Figure 7.8 (b)) as they do



(a) Reliability

(b) Efficiency

(c) Timeliness

Figure 7.8: Impact of number of information nodes on composite information ($R_d = 0.8$)

not adopt any information management mechanism. For ESRT and RBC all information nodes have to transport the information resulting in higher number of transmissions. Similarly, the latency of RBC and ESRT is higher than GIT for composite information which shows that GIT is more robust than RBC and ESRT (Figure 7.8 (c)).

7.3 Chapter Summary

In this chapter we evaluated the proposed framework for generic information transport (GIT) in WSNs. Through simulations we showed that GIT approach provides the desired application reliability despite evolving application requirements and dynamic network conditions. GIT reduces application dependency by utilizing generic information abstraction and its ability to tune itself according to application requirements. It is shown that the pro-

posed solution efficiently reduces the information redundancy. For certain type of information, 4-5 times lower number of transmissions is required to fulfill desired application reliability compared to state of the art solutions. GIT copes with a wide range of network conditions ranging from basic wireless links to network wide congestion by adapting between basic temporal and spatial reliability mechanisms. The simulation results confirm the capability of GIT to tune according to the application requirements and maintain the desired reliability. Furthermore, it is also shown that GIT performs equally well when information from all sensor nodes is required by the application.

Chapter 8

Conclusions and Future Research

In this thesis we developed a generic framework for assuring tunable reliability of information transport in Wireless Sensor Networks (WSNs). This chapter concludes the thesis by summarizing our main contributions and discussing their extendability. In this light, we sketch possible extensions of our framework for mobile WSNs, where mobility can be exploited to enhance the information transport in WSNs. We believe that the work presented in this thesis opens up new interesting research directions. Therefore, this chapter discusses the key issues and presents ideas to expand our framework.

8.1 Overall Thesis Contributions

The main goal of the thesis was to develop a framework and generic mechanisms to support tunable reliability of information transport in WSNs. Our research effort was driven by the current need of generic solution for information transport to fulfill evolving application requirements and dynamic network conditions. Accordingly, this section discusses the key contributions driven by the research questions listed in Section 1.4.1.

8.1.1 Analytical Modeling and Comparison

In order to understand the dynamics of information transport, this thesis has developed a new and abstract analytical modeling technique. The introduced analytical modeling is based on the reliability block diagrams (RBDs). The model is general enough to be representative for the existing semantics of data transport in WSNs. RBD models present an elegant way to describe and discover important trends and help in determining the sub-parameters either by performing further analytical work or by using simulations. Furthermore, the proposed modeling technique provides easy adaptation of different protocol parameters according to the desired application requirements. Consequently, we used the results for a better understanding of the impact of relevant parameters on the performance of the modeled protocols. The RBD modeling in discussion was presented in depth in Chapter 3.

As an inherent development following the analytical modeling of the information transport, in the same chapter we have compared the state-of-the-art data transport protocols. The comparative study quantifies the certainty of the analytical modeling. Furthermore, the comparison of different data transport protocols highlights the pros and cons of the existing data transport strategies.

Overall, the development of the analytical models and the highlighting of the deficiencies of existing solutions using the comparative study represent the contribution **C1** of our work, as defined in the introductory chapter of this thesis (Section 1.4.2).

Resultant publication

- **Faisal Karim Shaikh**, Abdelmajid Khelil, Neeraj Suri *On Modeling the Reliability of Data Transport in Wireless Sensor Networks*, In Proceedings of Euromicro Conference on Parallel, Distributed and Network-based Processing (PDP), pp. 395-402, 2007.

- **Faisal Karim Shaikh**, Abdelmajid Khelil, Neeraj Suri, *Poster: Meeting the Evolving Reliability Requirements for WSN Applications* In Proceedings of European Conference on Wireless Sensor Networks (EWSN), 2007.

- **Faisal Karim Shaikh**, Abdelmajid Khelil and Neeraj Suri, *A Comparative study of Data Transport Protocols in Wireless Sensor Networks*, Proceedings of IEEE International Symposium on World of Wireless, Mobile and Multimedia Networks (WOWMOM), pp. 1-9, 2008.

8.1.2 Generic Framework for Information Transport

The main contribution of this thesis is a generalized information transport framework for WSNs. Our framework efficiently provides tunable reliability of information transport using adaptive retransmissions, hybrid acknowledgment and opportunistically suppressing the information. Furthermore, our framework proactively monitors the congestion in the network and maintains the desired reliability by adapting the split path technique. In Chapter 4, we detail the modular architecture of the generic information transport framework. We identify that for efficient information transport it is necessary to manage and select the appropriate sensor nodes. Accordingly, the same chapter contains our proposed techniques for selecting the subset of sensor nodes generating different types of information.

Chapter 5 describes several techniques for different modules of the framework. More specifically, this chapter exploits spatial correlation of information and provides tunable reliability using adaptive retransmissions based on spatial correlation. In order to maintain the tunable reliability we propose reliability allocation technique along the path of information flow. To recover information loss an implicit acknowledgment scheme is utilized.

Enhancing the proposed techniques, Chapter 6 presents congestion aware tunable reliability of information transport. We propose proactive congestion detection mechanism compared to the existing reactive mechanisms. We identify three types of congestions in WSNs, i.e., link level, short lived and long lived congestion. Accordingly, we propose efficient solutions to overcome the congestion and maintain the desired application reliability. For information loss recovery we enhanced the implicit acknowledgment scheme and propose hybrid acknowledgment mechanism. Hybrid acknowledgement technique along with adaptive retransmission timer results in efficiently achieving the tunable reliability of information transport, i.e., using less number of transmissions.

Finally, in Chapter 7 several experimental studies are conducted to evaluate the proposed generic framework. The experimental results show the tunability aspects of the proposed framework for different types of information. The framework achieves the desired application reliability with less number of transmissions compared to state of the art solutions. For certain type of information, i.e., redundant atomic information, the framework achieves up to 4-5 times reduction in number of transmissions. Although, our solution does not provide timeliness guarantees, the results reveal that the latency of the proposed framework is low corresponding to existing solutions.

From the above observations, we conclude that our proposed framework simplifies the information transport in WSNs, since it supports different applications with evolving reliability requirements, copes with dynamic network properties and tolerates major perturbations.

Concluding, the generic information transport framework proposed in this thesis (Chapters 4, 5, 6) along with the extensive evaluation (Chapter 7) represents the thesis contributions **C2**, **C3**, **C4** and **C5**. For a detailed description of these contributions, see Section 1.3 and Section 1.4.2 of this thesis.

Resultant publications

- **Faisal Karim Shaikh**, Abdelmajid Khelil, Azad Ali and Neeraj Suri, *ReCAIT: Reliable Congestion Aware Information Transport in Wireless Sensor Networks*, submitted to International Journal of Communication Networks and Distributed Systems, a Special issue "Scalable Wireless Networks", 2010. (under review)

- **Faisal Karim Shaikh**, Abdelmajid Khelil, Brahim Ayari, Piotr Szczytowski and Neeraj Suri, *Generic Information Transport for Wireless Sensor Networks*, Proceedings of the third IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing (SUTC), June 2010. (to appear)

- **Faisal Karim Shaikh**, Abdelmajid Khelil, Azad Ali and Neeraj Suri, *TRCCIT: Tunable Reliability with Congestion Control for Information Transport in Wireless Sensor Networks*, Proceedings of the International Wireless Internet Conference (WICON), 2010.

- **Faisal Karim Shaikh**, Abdelmajid Khelil and Neeraj Suri, *AReIT: Adaptable Reliable Information Transport for Service Availability in Wireless Sensor Networks*, Proceedings of The International Conference on Wireless Networks (ICWN), pp. 75-81, 2009.

8.2 Extension of the Framework for Mobility Assisted WSNs

Recently, different system models are incorporated in traditional WSNs to enhance its functionality. Typical for such scenarios is that mobile nodes cooperate side-by-side with static sensor nodes to monitor the area of interest and to support the core network operations such as information collection [Jun et al., 2005; Shah et al., 2003; Wang et al., 2007b; Zhao et al., 2004]. The monitoring of environment constitutes a key application of WSNs. As a preliminary effort we consider only the monitoring application class for the extension of our framework. Generally, for non critical monitoring applications the latency of data collection is relaxed. Accordingly, we developed efficient schemes to monitor the physical environment which exploits the delay tolerance of the applications. An emerging diagnostic schema entails creating WSN wide maps of interested attributes [Khelil et al., 2008] called as global maps (gMap). In [Khelil et al., 2009, 2010], we have presented an extremely efficient mobility-assisted approach termed as gMAP to construct delay tolerant global maps. In gMAP (a) sensor nodes do not need to process readings of other nodes and (b) require to communicate a minimal number of messages compared to the existing approaches. This is achieved by opportunistically exploiting node mobility to collect information, keeping the sensor nodes transmit only their own readings on-demand to a mobile node in their transmission area. The mobile nodes traverse in the WSN and collect the information opportunistically and according to application requirements. We develop efficient movement algorithms for information collection. To ensure reliability we utilize stop and wait strategy where mobile node stops at the designated points inside the network and collects the information according to the application requirements. We verify the collection scheme using different types of mobility patterns and show that tunable reliability can be achieved in mobility assisted WSNs.

Resultant publications

- Piotr Szczytowski, **Faisal Karim Shaikh**, Vinay Sachidananda, Abdelmajid Khelil and Neeraj Suri, *Mobility Assisted Adaptive Sampling in Wireless Sensor Networks*, In Proceedings of the International Conference on Networked Sensing Systems (INSS), Demo Session, 2010. (to appear)

- Abdelmajid Khelil, **Faisal Karim Shaikh**, Azad Ali, Neeraj Suri and Christian Reinl, *Delay-Tolerant Monitoring of Mobility-Assisted Wire-*

less Sensor Networks, In "Delay Tolerant Networks: Protocols and Applications", Auerbach Publications, CRC Press, Taylor & Francis Group, Edited by A. Vasilakos, Y. Zhang, T. Spyropoulos (to appear 2010)

- Abdelmajid Khelil, **Faisal Karim Shaikh**, Azad Ali and Neeraj Suri, *gMAP: Efficient Construction of Global Maps for Mobility-Assisted Wireless Sensor Networks*, Proceedings of Conference on Wireless On demand Network Systems and Services (WONS), pp. 189-196, 2009.

8.3 Open Ends - Basis for Future Work

The work presented in this thesis addressed the posed research questions and discussed the resulting contributions. While addressing the research questions, this thesis also opened new and interesting research perspectives along its way. In the following, we briefly present some of the most promising ones.

Guaranteeing Timeliness: Despite the fact that our solution provide low latency in most of the cases, for real time applications timeliness guarantee is necessary. Therefore, developing efficient solution which provide tunable reliability and fulfills timeliness requirements is needed.

Supporting Duty Cycles: To conserve energy in WSNs, letting few or all sensor nodes in sleep state represents a promising technique for a certain class of application, i.e., monitoring. Sleeping of sensor nodes can be viewed by our approach as disruptions along the path to transport the information. A potential research direction will be exploring either existing routing solutions for duty cycled WSNs are sufficient to be utilized by the framework or appropriate mechanisms should be developed to ensure tunable reliability of information transport.

Application to Heterogeneous WSNs: As a preliminary effort we have started to explore the possibilities of using our framework for mobility assisted WSNs. Alongside mobility, heterogeneous sensing as well heterogeneous mobile nodes can be a part of WSNs. It is worth investigating to include different modules in our framework which keeps the heterogeneity of the environment and devices intact while providing application specific reliability.

Incorporating other Failure Models: Although our framework tolerates the major perturbations hindering the information transport, one of the

research questions we plan to further investigate is how the intolerable faults can be handled, e.g., partitioning. A possible solution might be to exploit the mobility (if available) to connect the different partitions of WSNs. Furthermore, security in WSNs is gaining importance and eventually information transport mechanisms have to incorporate techniques that cope with malicious sensor nodes. Therefore, we envision that incorporating security mechanisms in information transport paradigm is inevitable.

Real World Implementation: The implementation of the proposed framework on testbed and or deployment in real world scenario would be a significant contribution towards the WSN community. The real world implementation will provide more insights and might offer room for further improvements in the proposed framework.

Bibliography

A. A. Abbasi and M. Younis. A survey on clustering algorithms for wireless sensor networks. *Comput. Commun.*, 30(14-15):2826–2841, 2007.

H. M. F. AboElFotoh, S. S. Iyengar, and K. Chakrabarty. Computing reliability and message delay for cooperative wireless distributed sensor networks subject to random failures. *IEEE Transactions on Reliability*, 54(1): 145–155, 2005.

I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci. Wireless sensor networks: a survey. *Computer Networks*, 38(4):393–422, 2002.

J. N. Al-Karaki and A. E. Kamal. Routing techniques in wireless sensor networks: a survey. *IEEE Wireless Communications*, 11:6–28, 2004.

A. Ali, A. Khelil, F. K. Shaikh, and N. Suri. Efficient predictive monitoring of wireless sensor networks. *International Journal of Autonomous and Adaptive Communications Systems (IJAACS) (to appear)*, 2010.

A. Arora, P. Dutta, S. Bapat, and V. K. et al. A line in the sand: a wireless sensor network for target detection, classification, and tracking. *Computer Networks*, 46(5):605–634, 2004.

N. Baccour, A. Koubâa, M. B. Jamâa, H. Youssef, M. Zuniga, and M. Alves. A comparative simulation study of link quality estimators in wireless sensor networks. In *International Symposium on Modelling, Analysis and Simulation of Computer and Telecommunication Systems (MASCOTS 2009)*, 2009.

D. Bein, V. Jolly, B. Kumar, and S. Latifi. Reliability modeling in wireless sensor networks. *International Journal of Information Technology*, 11(2): 1–8, 2005.

M. Caleffi, G. Ferraiuolo, and L. Paura. A reliability-based framework for multi-path routing analysis in mobile ad-hoc networks. *International Jour-*

nal of Communication Networks and Distributed Systems, 1(4-5-6):507–523, 2008.

A. Cerpa, J. Elson, M. Hamilton, J. Zhao, D. Estrin, and L. Girod. Habitat monitoring: application driver for wireless communications technology. In *Workshop on Data communication in Latin America and the Caribbean (SIGCOMM)*, pages 20–41, 2001.

R. Chellappa, G. Qian, and Q. Zheng. Vehicle detection and tracking using acoustic and video sensors. In *Proceedings of the International Conference on Acoustics, Speech and Signal Processing(ICASSP)*, pages 793–796, 2004.

S. Chen and N. Yang. Congestion avoidance based on lightweight buffer management in sensor networks. *IEEE Trans. Parallel Distrib. Syst.*, 17 (9):934–946, 2006.

W. Choi and S. K. Das. Coverage-adaptive random sensor scheduling for application-aware data gathering in wireless sensor networks. *Computer Communications*, 29(17):3467 – 3482, 2006.

W. Choi and S. K. Das. CROSS: A probabilistic constrained random sensor selection scheme in wireless sensor networks. *Performance Evaluation*, 2009.

Y. Choi, M. G. Gouda, H. Zhang, and A. Arora. Routing on a logical grid in sensor networks. In *Technical Report TR04-49, Department of Computer Sciences, The University of Texas at Austin*, 2004.

Y. Choi, M. G. Gouda, H. Zhang, and A. Arora. Stabilization of grid routing in sensor networks. *Journal of Aerospace Computing, Information and Communication*, 3:214–233, 2006.

S. Coleri-Ergen and P. Varaiya. Pedamacs: Power efficient and delay aware medium access protocol for sensor networks. *IEEE Transactions on Mobile Computing*, 5(7):920–930, 2006.

D. Couto, D. Aguayo, J. Bicket, and R. Morris. A high-throughput path metric for multi-hop wireless routing. *Wireless Networks*, 11(4):419–434, 2005.

B. Deb, S. Bhatnagar, and B. Nath. Information assurance in sensor networks. In *In Proceedings of the ACM Conference on Wireless Sensor Networks and Applications (WSNA)*, pages 160–168, 2003a.

B. Deb, S. Bhatnagar, and B. Nath. Reinform: Reliable information forwarding using multiple paths in sensor networks. In *Proceedings of the 28th Annual IEEE International Conference on Local Computer Networks (LCN)*, pages 406–415, 2003b.

F. Delicato, P. Pires, L. Pinnez, L. Fernando, and L. da Costa. A flexible web service based architecture for wireless sensor networks. In *International Conference on Distributed Computing Systems Workshops*, pages 730–735, 2003.

T. L. Dinh, W. Hu, P. Sikka, P. Corke, L. Overs, and S. Brosnan. Design and deployment of a remote robust sensor network: Experiences from an outdoor water quality monitoring network. In *Proceedings of the 32nd IEEE Conference on Local Computer Networks (LCN)*, pages 799–806, 2007.

W. Dong, C. Chen, X. Liu, J. Bu, and Y. Liu. Performance of bulk data dissemination in wireless sensor networks. In *DCOSS '09: Proceedings of the 5th IEEE International Conference on Distributed Computing in Sensor Systems*, pages 356–369, 2009.

C. T. Ee and R. Bajcsy. Congestion control and fairness for many-to-one routing in sensor networks. In *Proceedings of the 2nd international conference on Embedded networked sensor systems (SenSys)*, pages 148–161, 2004.

E. Fasolo, M. Rossi, J. Widmer, and M. Zorzi. In-network aggregation techniques for wireless sensor networks: a survey. *Wireless Commun.*, 14(2): 70–87, 2007.

E. Felemban, C.-G. Lee, and E. Ekici. Mmspeed: Multipath multi-speed protocol for qos guarantee of reliability and timeliness in wireless sensor networks. *IEEE Transactions on Mobile Computing*, 5(6):738–754, 2006. ISSN 1536-1233.

G. Fox, A. Ho, R. Wang, E. Chu, and I. Kwan. A collaborative sensor grids framework. In *International Symposium on Collaborative Technologies and Systems (CTS)*, pages 29–38, 2008.

D. Ganesan, R. Govindan, S. Shenker, and D. Estrin. Highly-resilient, energy-efficient multipath routing in wireless sensor networks. *SIGMOBILE Mob. Comput. Commun. Rev.*, 5(4):11–25, 2001. ISSN 1559-1662.

Y. Gu, D. Bozdag, E. Ekici, F. Ozguner, and C.-G. Lee. Partitioning based mobile element scheduling in wireless sensor networks. In *Proceedings of the 2nd IEEE Communications Society Conference on Sensor and Ad Hoc Communications and Networks (SECON)*, pages 386–395, 2005.

L. Guang-Hui, Z. Jun, and W. Zhi. Research on forest fire detection based on wireless sensor network. In *Proceedings of the World Congress on Intelligent Control and Automation*, pages 275–279, 2006.

C. Hartung, R. Han, C. Seielstad, and S. Holbrook. FireWxNet: a multi-tiered portable wireless system for monitoring weather conditions in wildland fire environments. In *Proceedings of the 4th international conference on Mobile systems, applications and services*, pages 28–41, 2006.

T. He, F. Ren, C. Lin, and S. Das. Alleviating congestion using traffic-aware dynamic routing in wireless sensor networks. In *Conference on Sensor, Mesh and Ad Hoc Communications and Networks (SECON)*, pages 233–241, 2008.

J. M. Hellerstein, W. Hong, and S. Madden. Beyond average: Toward sophisticated sensing with queries. In *International Workshop on Information Processing in Sensor Networks (IPSN)*, pages 63–79, 2003.

C.-W. Hsu, C.-S. Shieh, and W. K. Lai. A multi-path routing protocol with reduced control messages for wireless sensor networks. In *International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP)*, pages 671–675, 2007.

B. Hull, K. Jamieson, and H. Balakrishnan. Mitigating congestion in wireless sensor networks. In *Proc. of ACM SenSys*, pages 134 – 147, 2004a.

B. Hull, K. Jamieson, and H. Balakrishnan. Mitigating Congestion in Wireless Sensor Networks. In *Proceedings of the international conference on Embedded networked sensor systems (SenSys)*, pages 134 – 147, Baltimore, MD, November 2004b.

C. Intanagonwiwat, R. Govindan, D. Estrin, J. Heidemann, and F. Silva. Directed diffusion for wireless sensor networking. *IEEE/ACM Trans. Netw.*, 11:2–16, 2003.

Y. G. Iyer, S. Gandham, and S. Venkatesan. Stcp: A generic transport layer protocol for wireless sensor networks. In *International Conference on Computer Communications and Networks (ICCCN)*, pages 449 – 454, 2005.

V. Jacobson. Congestion avoidance and control. In *Symposium proceedings on Communications architectures and protocols (SIGCOMM)*, pages 314–329, 1988.

K. Jaewon, Z. Yanyong, and B. Nath. Tara: Topology-aware resource adaptation to alleviate congestion in sensor networks. *IEEE Transactions on Parallel and Distributed Systems*, 18(7):919–931, 2007.

H. Jun, M. H. Ammar, and E. W. Zegura. Power management in delay tolerant networks: a framework and knowledge-based mechanisms. In *Second Annual IEEE Communications Society Conference on Sensor and Ad Hoc Communications and Networks (SECON)*, pages 418–429, 2005.

K. Karenos, V. Kalogeraki, and S. V. Krishnamurthy. Cluster-based congestion control for sensor networks. *ACM Trans. Sen. Netw.*, 4(1):1–39, 2008.

F. Karim, A. Khelil, and N. Suri. On modeling the reliability of data transport in wireless sensor networks. In *The Fifteen Euromicro Conference on Parallel, Distributed and Network-based Processing*, pages 395–402, 2007.

H. Karl and A. Willig. *Protocols and Architectures for Wireless Sensor Networks*. John Wiley & Sons, 2005. ISBN 0470095105.

A. Khelil, F. Shaikh, B. Ayari, and N. Suri. MWM: A Map-based World Model for Wireless Sensor Networks. In *Proc. of The 2nd ACM International Conference on Autonomic Computing and Communication Systems (AUTONOMICS)*, 2008.

A. Khelil, F. K. Shaikh, A. Ali, and N. Suri. gMAP: an efficient construction of global maps for mobility-assisted wireless sensor networks. In *Conference on Wireless On demand Network Systems and Services (WONS)*, pages 189–196, 2009.

A. Khelil, F. K. Shaikh, A. Ali, N. Suri, and C. Reinl. *Delay Tolerant Networks: Protocols and Applications*, chapter Delay-Tolerant Monitoring of Mobility-Assisted Wireless Sensor Networks. Auerbach Publications, CRC Press, Taylor & Francis Group, 2010.

S. Kim, R. Fonseca, P. Dutta, A. Tavakoli, D. Culler, P. Levis, S. Shenker, and I. Stoica. Flush: a reliable bulk transport protocol for multihop wireless networks. In *Proceedings of the 5th international conference on Embedded networked sensor systems (SenSys)*, pages 351–365, 2007.

J. Kulik, W. Heinzelman, and H. Balakrishnan. Negotiationbased protocols for disseminating information in wireless sensor networks. In *ACM MobiCom (MobiCom)*, 1999.

M. Kuorilehto, M. Hännikäinen, and T. D. Hämäläinen. A survey of application distribution in wireless sensor networks. *EURASIP J. Wirel. Commun. Netw.*, 2005(5):774–788, 2005.

K. Langendoen. Medium access control in wireless sensor networks. In H. Wu and Y. Pan, editors, *Medium Access Control in Wireless Networks*, pages 535–560. Nova Science Publishers, Inc., may 2008.

T. Lea, W. Hub, P. Corkeb, and S. Jhaa. ERTP: energy-efficient and reliable transport protocol for data streaming in wireless sensor networks. *Computer Communications*, 32(7-10):1154–1171, 2009.

S.-J. Lee and M. Gerla. Split multipath routing with maximally disjoint paths in ad hoc networks. In *International Conference on Communications (ICC)*, 2001.

P. Levis, N. Lee, M. Welsh, and D. Culler. TOSSIM: accurate and scalable simulation of entire tinyos applications. In *Proceedings of the International Conference on Embedded Networked Sensor Systems (SenSys)*, pages 126–137, 2003.

H. B. Lim, Y. M. Teo, P. Mukherjee, V. T. Lam, W. F. Wong, and S. See. Sensor grid: Integration ofwireless sensor networks and the grid. In *IEEE Conference on Local Computer Networks (LCN)*, pages 91–98, 2005.

U. Malesci and S. Madden. A measurement-based analysis of the interaction between network layers in tinyos. In *Third European Workshop on Wireless Sensor Networks*, pages 292–309, 2006.

B. Marchi, A. Grilo, and M. S. Nunes. Dtsn: Distributed transport for sensor networks. In *Proceedings of the 12th IEEE Symposium on Computers and Communications (ISCC)*, pages 165–172, 2007.

A. Oka and L. Lampe. Energy efficient distributed filtering with wireless sensor networks. *IEEE Transactions on Signal Processing*, 56(5):2062–2075, 2008.

J. Paek and R. Govindan. Rcrt: rate-controlled reliable transport for wireless sensor networks. In *SenSys*, pages 305–319, 2007.

S. Park, R. Vedantham, R. Sivakumar, and I. F. Akyildiz. A scalable approach for reliable downstream data delivery in wireless sensor networks. In *Proceedings of the Interational Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc)*, pages 78–89, 2004.

J. Polastre, J. Hill, and D. Culler. Versatile low power media access for wireless sensor networks. In *Proceedings of the International Conference on Embedded Networked Sensor Systems (SenSys)*, pages 95–107, 2004.

J. Polastre, R. Szewczyk, and D. Culler. Telos: enabling ultra-low power wireless research. In *Proceedings of the 4th international symposium on Information processing in sensor networks (IPSN)*, 2005.

L. Popa, C. Raiciu, I. Stoica, and D. Rosenblum. Reducing congestion effects in wireless networks by multipath routing. In *Proceedings of the IEEE International Conference on Network Protocols (ICNP)*, pages 96–105, 2006.

M. A. Rahman, A. E. Saddik, and W. Gueaieb. Wireless sensor network transport layer: State of the art. In S. Mukhopadhyay and R. Huang, editors, *Sensors: Advancement In Modeling, Design Issues, Fabrication And Practical Applications*, volume 21 of *LECTURE NOTES IN ELECTRICAL ENGINEERING*, pages 221–245. Springer-Verlag, 2008.

V. Rajendran, K. Obraczka, and J. Garcia-Luna-Aceves. Energy-efficient, collision-free medium access control for wireless sensor networks. In *The ACM Conference on Embedded Networked Sensor Systems*, 2003.

S. Rangwala, R. Gummadi, R. Govindan, and K. Psounis. Interference-aware fair rate control in wireless sensor networks. *SIGCOMM Comput. Commun. Rev.*, 36(4):63–74, 2006.

Y. Sankarasubramaniam, Ö. B. Akan, and I. F. Akyildiz. Esrt: event-to-sink reliable transport in wireless sensor networks. In *Interational Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc)*, pages 177–188, 2003.

O. Saukh, P. J. Marrón, A. Lachenmann, M. Gauger, D. Minder, and K. Rothermel. Generic routing metric and policies for wsns. In *Proceedings of the European Workshop on Wireless Sensor Networks (EWSN)*, pages 99–114, 2006.

L. Selavo, A. Wood, Q. Cao, T. Sookoor, H. Liu, A. Srinivasan, Y. Wu, W. Kang, J. Stankovic, D. Young, and J. Porter. LUSTER: Wireless sensor network for environmental research. In *Proceedings of the 5th international*

conference on Embedded networked sensor systems (SenSys), pages 103–116, 2007.

R. C. Shah, S. Roy, S. Jain, and W. Brunette. Data mules: modeling and analysis of a three-tier architecture for sparse sensor networks. *Ad Hoc Networks*, 1(2-3):215–233, 2003.

F. K. Shaikh, A. Khelil, and N. Suri. A comparative study for data transport protocols for wsn. In *IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks (WOWMOM)*, pages 1 – 9, 2008.

K.-P. Shih, S.-S. Wang, H.-C. Chen, and P.-H. Yang. Collect: Collaborative event detection and tracking in wireless heterogeneous sensor networks. *Computer Communications*, 31(14):3124–3136, 2008.

A. Shrestha, L. Xing, and H. Liu. Modeling and evaluating the reliability of wireless sensor networks. In *Annual Reliability and Maintainability Symposium (RAMS)*, pages 186 –191, 2007.

I. Solis and K. Obraczka. Isolines: energy-efficient mapping in sensor networks. In *IEEE Symposium on Computers and Communications (ISCC)*, pages 379– 385, 2005.

F. Stann and J. Heidemann. Rmst: Reliable data transport in sensor networks. In *Proceedings of the First International Workshop on Sensor Net Protocols and Applications*, pages 102–112, 2003.

M. Strasser, A. F. Meier, K. Langendoen, and P. Blum. Dwarf: Delay-aware robust forwarding for energy-constrained wireless sensor networks. In *Proceedings of the 3rd IEEE International Conference on Distributed Computing in Sensor Systems (DCOSS 2007)*, pages 64–81, June 2007.

R. Szewczyk, E. Osterweil, J. Polastre, M. Hamilton, A. Mainwaring, and D. Estrin. Habitat monitoring with sensor networks. *ACM Communication*, 47(6):34–40, 2004.

J.-Y. Teo, Y. Ha, and C.-K. Tham. Interference-minimized multipath routing with congestion control in wireless sensor network for high-rate streaming. *IEEE Transactions on Mobile Computing*, 7(9):1124–1137, 2008.

N. Tezcan and W. Wang. Art: an asymmetric and reliable transport mechanism for wireless sensor networks. *Int. J. Sen. Netw.*, 2(3/4):188–200, 2007.

TinyAODV. `http://cvs.sourcefourge.net/viewcvs.py/tinyos/tinyos-1.x/contrib/hsn/`, 2003.

TinyOS. `http://tinyos.net/`, 1999.

S. Vinga. *Resiliency Assessment of Wireless Sensor Networks: A Holistic Approach*. PhD thesis, FEDERICO II, UNIVERSITY OF NAPLES, 2009.

P. Völgyesi, A. Nadas, A. Ledeczi, and K. Molnar. Reliable multihop bulk transfer service for wireless sensor networks. In *International Symposium and Workshop on Engineering of Computer Based Systems*, pages 112–122, 2006.

M. C. Vuran, O. B. Akan, and I. F. Akyildiz. Spatio-temporal correlation: Theory and applications for wireless sensor networks. *Computer Networks Journal (Elsevier)*, 45(3):245 –259, 2004.

M. C. Vuran, V. C. Gungor, and O. B. Akan. On the interdependence of congestion and contention in wireless sensor networks. In *Workshop on Measurement, Modeling, and Performance Analysis of Wireless Sensor Networks (SenMetrics)*, 2005.

C. J. Walter and N. Suri. The customizable fault/error model for dependable distributed systems. *Journal of Theoretical Computer Science*, 290(2): 1223–1251, 2003.

C. Wan, A. T. Campbell, and L. Krishnamurthy. Psfq: a reliable transport protocol for wireless sensor networks. In *International Workshop on Wireless Sensor Networks and Applications (WSNA)*, pages 1–11, 2002.

C.-Y. Wan, S. B. Eisenman, and A. T. Campbell. CODA: congestion detection and avoidance in sensor networks. In *Proceedings of the International Conference on Embedded Networked Sensor Systems*, pages 266–279, 2003.

C. Wang, M. Daneshmand, B. Li, and K. Sohraby. A survey of transport protocols for wireless sensor networks. *IEEE Network Magazine, Special Issue on Wireless Sensor Networking*, 20(3):34–40, 2006a.

C. Wang, K. Sohraby, V. Lawrence, B. Li, and Y. Hu. Priority-based congestion control in wireless sensor networks. *Sensor Networks, Ubiquitous, and Trustworthy Computing, International Conference on*, 1:22–31, 2006b.

C. Wang, K. Sohraby, B. Li, M. Daneshmand, and Y. Hu. A survey of transport protocols for wireless sensor networks. *IEEE Network*, 20(3): 34–40, 2006c.

C. Wang, K. Sohraby, V. Lawrence, B. Li, and Y. Hu. Upstream congestion control in wireless sensor networks through cross-layer optimization. *IEEE Journal on Selected Areas in Communications*, 25(4):786–798, 2007a.

Y. Wang, H. Dang, and H. Wu. A survey on analytic studies of delay-tolerant mobile sensor networks. *Journal of Wireless Communications and Mobile Computing (WCMC) Special Issue on Disruption Tolerant Networking for Mobile or Sensor Networks*, 7(10):1197–1208, 2007b.

G. Werner-Allen, K. Lorincz, M. Welsh, O. Marcillo, J. Johnson, M. Ruiz, and J. Lees. Deploying a wireless sensor network on an active volcano. *IEEE Internet Computing*, 10(2):18–25, 2006.

A. Willig and H. Karl. Data transport reliability in wireless sensor networks – a survey of issues and solutions. *Praxis der Informationsverarbeitung und Kommunikation*, 28:86–92, 2005.

A. Woo, T. Tong, and D. Culler. Taming the underlying challenges of reliable multihop routing in sensor networks. In *Proceedings of the International Conference on Embedded Networked Sensor Systems (SenSys)*, pages 14–27, 2003.

L. Xing and A. Shrestha. Qos reliability of hierarchical clustered wireless sensor networks. In *International Performance, Computing, and Communications Conference (IPCCC)*, pages 641–646, 2006.

N. Xu, S. Rangwala, K. K. Chintalapudi, D. Ganesan, A. Broad, R. Govindan, and D. Estrin. A wireless sensor network for structural monitoring. In *Proceedings of the 2nd international conference on Embedded networked sensor systems (SenSys)*, pages 13–24, 2004.

W. Ye, J. Heidemann, and D. Estrin. Medium access control with coordinated adaptive sleeping for wireless sensor networks. *Transactions on Networking*, pages 493–506, 2004a.

W. Ye, J. Heidemann, and D. Estrin. Medium access control with coordinated adaptive sleeping for wireless sensor networks. *IEEE/ACM Trans. Netw.*, 12(3):493–506, 2004b.

Y. Yu, L. J. Rittle, V. Bhandari, and J. B. LeBrun. Supporting concurrent applications in wireless sensor networks. In *Proceedings of the 4th international conference on Embedded networked sensor systems (SenSys)*, pages 139–152, 2006.

H. Zhang, A. Arora, Y. Choi, and M. G. Gouda. Reliable bursty convergecast in wireless sensor networks. In *Interational Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc)*, pages 266–276, 2005.

J. Zhao and R. Govindan. Understanding packet delivery performance in dense wireless sensor networks. In *International Conference on Embedded Networked Sensor Systems (SenSys)*, pages 1–13, 2003.

W. Zhao, M. Ammar, and E. Zegura. A Message Ferrying Approach for Data Delivery in Sparse Mobile Ad Hoc Networks. In *Proceedings of ACM Mobihoc 2004*, May 2004.

Y. Zhou and M. R. Lyu. Port: A price-oriented reliable transport protocol for wireless sensor networks. In *International Symposium on Software Reliability Engineering*, pages 117–126, 2005.

Index

Curriculum Vitae

Personal Data

Name: Faisal Karim Shaikh

Date of birth: March 3rd, 1978

Place of birth: Matiari, Pakistan

School Education

May 1993 Matriculation from Board of Intermediate & Secondary Education, Hyderabad, Pakistan.

May 1995 Intermediate from Board of Intermediate & Secondary Education, Hyderabad, Pakistan.

University Education

1996-2001 *Bachelor of Engineering (Computer Systems)* – Mehran University of Engineering & Technology, Jamshoro, Pakistan. (secured 3rd position)

2001-2003 *Master of Engineering (Communication Systems and Networks)* – Mehran University of Engineering & Technology, Jamshoro, Pakistan.

2005-2010 *Ph.D. in Computer Science* – Technische Universität Darmstadt, Darmstadt, Germany.